



## Identiteetin- ja pääsynhallinta

### Citation

Linden, M. (2015). Identiteetin- ja pääsynhallinta. (Tampere University of Technology. Department of Pervasive Computing. Report; Vuosikerta 6). Tampere University of Technology.

### Year

2015

### Version

Publisher's PDF (version of record)

### Link to publication

TUTCRIS Portal (<http://www.tut.fi/tutcris>)

### Take down policy

If you believe that this document breaches copyright, please contact [cris.tau@tuni.fi](mailto:cris.tau@tuni.fi), and we will remove access to the work immediately and investigate your claim.

Mikael Linden

**Identiteetin- ja pääsynhallinta**



Mikael Linden

## **Identiteetin- ja pääsynhallinta**

ISBN 978-952-15-3568-0  
ISSN 2323-9174

# Identiteetin- ja pääsynhallinta

TkT Mikael Linden, CISSP

Tampereen teknillinen yliopisto

Tietotekniikan laitos

15.8.2015

## Sisällys

1.	Johdanto .....	4
2.	Hyödyistä ja haasteista.....	6
2.1.	Tietoturvallisuus.....	6
2.2.	Tehokkuus.....	7
2.3.	Uudet toimintatavat.....	8
2.4.	Haasteita.....	8
2.5.	Pohdittavaa.....	9
3.	Identiteetti .....	10
3.1.	Käsitteitä .....	10
3.2.	Attribuutit.....	11
3.3.	Yksilöivät tunnisteet .....	12
3.4.	Pseudonyymit eli salanimet .....	14
3.5.	Pohdittavaa.....	15
4.	Identiteetin todentaminen eli autentikointi .....	16
4.1.	Autentikoinnin määritelmä ja menetelmät.....	16
4.2.	Ensitunnistus ja tunnistuksen luotettavuus .....	17
4.3.	Tunnistuksen vahvuuden standardeja ja viitekehyksiä .....	20
4.4.	Keinoja tukevampaan salasanan tunnistukseen .....	21
4.5.	Julkisen avaimen järjestelmä, varmenteet ja toimikortit.....	22
4.6.	Biometrinen tunnistus .....	26
4.7.	Kertakirjautuminen .....	28
4.8.	Lopuksi.....	30
4.9.	Pohdittavaa.....	30
5.	Käyttövaltuuksien hallinta eli auktorisointi .....	31
5.1.	Määritelmä .....	31
5.2.	Pääsynvalvontamatriisi .....	32
5.3.	Rooliin perustuva pääsynvalvonta .....	32
5.4.	Muita pääsynvalvontamenetelmiä.....	34
5.5.	Vähimmän käyttövaltuuden periaate .....	36
5.6.	Vaarallisten työtehtävien eriyttäminen .....	36
5.7.	Delegointi.....	37
5.8.	Pohdittavaa.....	37

6.	Jäljitettävyyys ja raportointi.....	39
6.1.	Jäljitettävyyys.....	39
6.2.	Raportointi .....	39
7.	Identiteetinhallinta organisaatiossa .....	41
7.1.	Kokonaisarkkitehtuuri.....	41
7.2.	Toiminta-arkkitehtuuri .....	42
7.3.	Tietoarkkitehtuuri.....	43
7.4.	Järjestelmäarkkitehtuuri .....	46
7.5.	Teknologia-arkkitehtuuri .....	46
7.6.	LDAP-hakemisto .....	47
7.7.	Identiteetinhallintajärjestelmä.....	49
7.8.	Pohdittavaa.....	52
8.	Federoitu identiteetinhallinta .....	53
8.1.	Peruskäsitteet .....	54
8.2.	Federoidun identiteetinhallinnan hyötyjä.....	55
8.3.	Luottamus ja luottamusmallit.....	56
8.4.	Teknologioista.....	57
8.5.	Käyttäjäkeskeinen identiteetinhallinta .....	59
8.6.	Esimerkkejä federoidun identiteetinhallinnan palveluista .....	60
8.7.	Pohdittavaa.....	62
9.	Tietosuoja ja henkilötietolaki.....	63
9.1.	OECD:n tietosuojaperiaatteet ja tietosuojadirektiivi .....	63
9.2.	Suojaamisvelvoitteesta.....	64
9.3.	Henkilörekisteriseloste.....	64
9.4.	Loogisen rekisterin käsite .....	65
9.5.	Henkilötietojen luovutus kolmansiin maihin .....	65
9.6.	Pohdittavaa.....	66

## Lukijalle

Tämä kirja syntyi alkujaan Tampereen teknillisen yliopiston kurssille TIE-30500 "Identiteetin ja pääsynhallinta, 4 op", jonka aihepiiristä yhtenäistä suomenkielistä oppimateriaalia on muutoin saatavilla varsin niukasti. Esitän kiitokseni Jukka Koskiselalle, Arto Tuomelle ja Juuso Kuusiselle heidän kirjan sisältöön antamistaan kommentteista ja kehittämisehdotuksista.

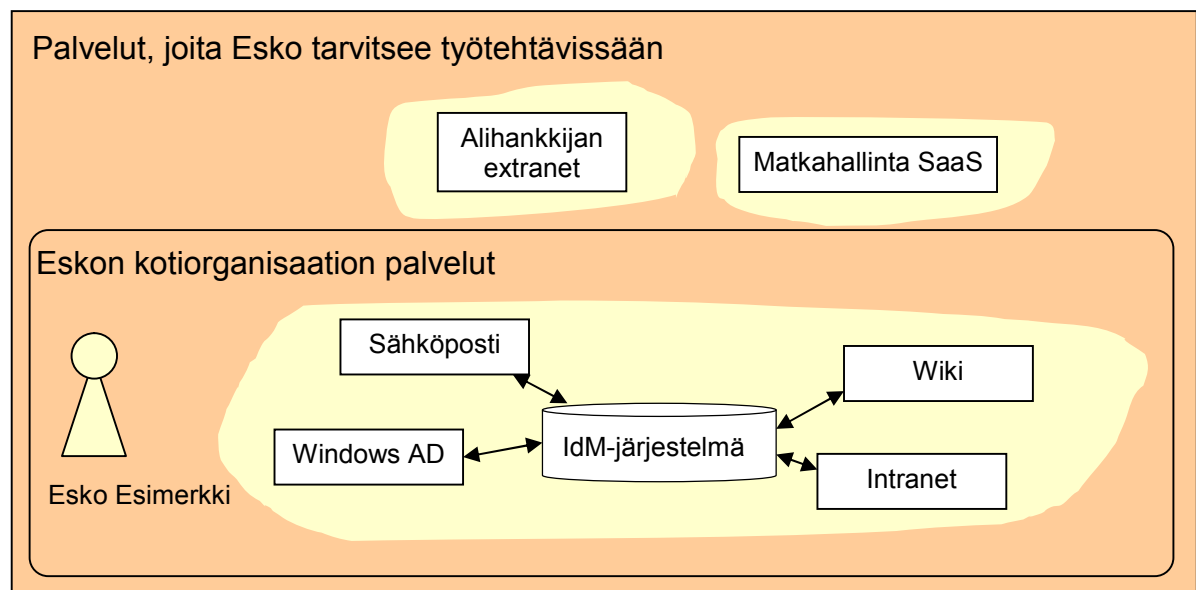
Tekijä

# 1. Johdanto

Käyttäjätunnukset ja niihin liittyvät salasanat ja käyttövaltuudet ovat tuttuja tietojärjestelmien ja -verkkojen käyttäjille. Yhdellä henkilöllä on lukuisia, toisistaan riippumattomia käyttäjätunnuksia palveluihin, joita hän käyttää toimiessaan jonkun organisaation jäsenenä (esimerkiksi työntekijänä, opiskelijana, asiakkaana, jopa tietyn valtion kansalaisena) tai yksityishenkilönä.

Identiteetin- ja pääsynhallinnan käsite alkoi muotoutua vuosituhaten vaihteessa, kun käyttäjän tunnistusta vaativien palveluiden määrä alkoi kasvaa. Kipupiste syntyi ensimmäisenä organisaatioympäristöön, jossa työntekijöille alkoi tulla lukuisia omaa elämäänsä eläviä käyttäjätunnuksia eri tietojärjestelmiin, kuten työasemiin ja palvelimiin, sähköpostiin ja intranetiin. Työntekijöiden käyttäjätunnusten avaaminen, sulkeminen ja unohtuneiden salasanoiden hallinta kävivät työläiksi, ja pian organisaatioissa havahduttiin myös niihin liittyviin tietoturvaongelmiin, kuten "roikkumaan jääneisiin" käyttäjätunnuksiin (työntekijän käyttäjätunnukset unohtetaan sulkea kun hänen palvelussuhteensa päättyy) ja salasana-tunnistuksen heikkouksiin.

IT-toimialalla alettiin kehittää tuotteita, joiden avulla käyttäjän käyttäjätunnuksia ("identiteettiä"), salasanoja ja käyttövaltuuksia ("pääsyä") voidaan hallita organisaatioissa aikaisempaa keskitetymmin, ja identiteetin- ja pääsynhallinnan (Identity and Access Management, IAM) tuoteperheet alkoivat muotoutua. Tuotteiden avustamana alettiin toteuttaa järjestelyjä (Kuva 1), joissa käyttäjällä on organisaatiossa yksi identiteetti, johon on kytketty mahdollisesti yksi käyttäjätunnus/salasana-pari. Tunnuksella käyttäjä voi kirjautua kaikkiin tai ainakin keskeisimpiin organisaation palveluihin, joihin hänellä on käyttövaltuus.



**Kuva 1. Keskitetty identiteettien hallinta organisaatiossa. Keltainen alue kuvastaa yhden identiteetin kattavuutta.**

Organisaatiossa identiteetin- ja pääsynhallinta on kuitenkin mitä suurimmassa määrin johtamisongelma; näppärinkään tekninen väline ei kykene auttamaan organisaatiota loppukäyttäjien käyttäjätunnusten ja käyttövaltuuksien hallinnassa, jos organisaatiossa ei ole ensin pystytty sopimaan riittävän määrämuotoisista toimintatavoista.



Yhdenmukaistamista tarvitaan esimerkiksi siinä, kuinka organisaatiossa ja sen eri tietojärjestelmissä ylläpidetään tietoa uusista ja päättyvistä palvelussuhteista tai erilaisten käyttövaltuuksien määräytymisen perusteista.

Tämä kirja käsittelee identiteetin- ja pääsynhallintaa pääasiassa organisaatiokeskeisesti. Tällöin käyttäjän identiteetin ylläpidosta huolehtii organisaatio, jossa käyttäjä on esimerkiksi työntekijänä, asiakkaana, opiskelijana tai potilaana. Organisaatiokeskeisen identiteetinhallinnan arkkityyppi on työntekijöidensä identiteettejä hallinnoiva työnantaja, koska organisaation työntekijöillä on paljon erilaisia käyttövaltuuksia, usein myös organisaation toiminnan kannalta sensitiivisiin palveluihin. Organisaatiokeskeisen identiteetinhallinnan vastakohtaa, käyttäjäkeskeistä identiteetinhallintaa, käsitellään lyhyesti luvussa 8.5.

Keskitettyyn identiteetinhallintaan organisaatioissa palataan luvussa 7, joka muodostaa keskeisen osuuden tätä kirjaa. Sitä ennen tutustutaan käsitteistöön, jonka ymmärtäminen on välttämätöntä eteenpäin lukemiselle. Luvussa 8 tutustutaan järjestelyihin, joilla käyttäjän identiteetti saadaan kattamaan usean eri organisaation ylläpitämiä verkkopalveluita (kuten Kuva 1:ssä ”Alihankkijan extranet” ja ”Matkahallinta SaaS”). Koska käyttäjän identiteetti on yleensä myös henkilötieto, luvussa 9 tutustutaan henkilötietojen käsittelyä säätelevään lainsäädäntöön Suomessa. Kirja alkaa kuitenkin tutustumisella identiteetin- ja pääsynhallinnan kehittämisestä saataviin hyötyihin ja sen haasteisiin.

## 2. Hyödyistä ja haasteista

Tässä luvussa esitetään näkökulmia identiteetin- ja pääsynhallinnan kehittämisestä saataviin hyötyihin. Näkökulmat on tiivistetty alla olevaan taulukkoon.

Näkökulma	Tavoite
Tietoturvallisuus	Riittävän suojauksen rakentaminen ja ylläpito mahdollisimman pienillä kustannuksilla. Suojausten kustannusten ja riskien tasapainottaminen.
Tehokkuus	Identiteetin- ja pääsynhallintaan tehtävillä panostuksilla pyritään kasvattamaan tehokkuutta, jolla edelleen tavoitellaan kustannussäästöjä ja/tai parempaa palvelutasoa.
Uudet toimintatavat	Identiteetin- ja pääsynhallinnan kehittämisellä pyritään mahdollistamaan sellaisia toimintamalleja tai liiketoimintatapoja, jotka eivät olisi mahdollisia muuten.

Taulukon näkökulmat eivät ole ristiriidassa keskenään, vaan samoja investointeja voidaan perustella useasta näkökulmasta. Toisaalta tehtäviä panostuksia voidaan painottaa kulloinkin tärkeästä näkökulmasta.

Näkökulmilla ei varsinaisesti ole tärkeysjärjestystä, mutta usein tietoturvallisuuteen liittyviä motiiveja kuitenkin korostetaan, koska organisaation toiminnan kannalta keskeisten suojattavien kohteiden vaarantuminen saattaa johtaa organisaation olemassaolon tai maineen vaarantumiseen. Organisaatio, jonka tietoturvallisuus on kunnossa mutta joka on tehoton eikä hyödynnä mahdollisia uusia toimintatapoja, ei ole yhtä välittömässä vaarassa kuin organisaatio, joka toimii tehokkaasti ja uusia toimintatapoja hyödyntäen, mutta jonka tietoturvallisuudessa on pahoja ongelmia.

### 2.1. Tietoturvallisuus

Erään määritelmän mukaan tietojärjestelmän turvallisuudella (computer security) tarkoitetaan käyttäjien valtuudettomien toimenpiteiden estämistä ja havaitsemista tietojärjestelmissä. Määritelmä lähestyy tietoturvallisuutta käyttäjien ja heidän käyttövaltuuksiensa kautta. Identiteetin- ja pääsynhallinnalla on siis tiiviit siteet tietoturvallisuuteen.

Identiteetinhallinnan perisynti on, että käyttäjän **käyttövaltuuksia ei muisteta poistaa, kun käyttövaltuuden peruste lakkaa**. Tyypillinen tilanne syntyy, kun työntekijä siirtyy toisen työnantajan palvelukseen, mutta hänen kaikkia käyttäjätunnuksiaan organisaation eri palveluissa ei muisteta sulkea (puhumattakaan tunnuksista organisaation ulkopuolella, esimerkiksi alihankkijan palveluissa). Jos käyttäjällä olisi vain yksi keskitetysti ylläpidetty käyttäjätunnus (vrt. Kuva 1), jonka sulkeminen katkaisee kaikki hänen käyttövaltuutensa eri palveluissa, voitaisiin tunnusten sulkemiseen liittyvät ponnistelut kohdentaa yhteen keskitettyyn paikkaan. Näin tunnus saadaan luotettavammin suljetuksi.

Jos käyttäjällä on erillinen identiteetti jokaisessa palvelussa, käyttäjän **muistia rasittavien salasanojen määrä kasvaa** siinä määrin, että käyttäjä joutuu lopulta kirjoittamaan salasanansa ylös. Monitoriin liimattu tai näppäimistön alle piilotettu muistilappu on klassinen esimerkki käytännöstä, jossa loppukäyttäjän mukavuudenhalu nakertaa

tietoturvallisuutta. Käyttäjä voi toki oma-aloitteisesti asettaa jokaiseen erilliseen tunnukseensa saman salasanan, mutta tällöin salasanan paljastumisen riski kasvaa ja sen säännöllinen uusiminen käy myös vaikeaksi. Identiteetin- ja pääsynhallinnan kehittämisessä pyritään tyypillisesti järjestelyyn, jossa samalla käyttäjätunnuksella ja salasanalla aukeaa suuri joukko palveluita. Toisaalta; jos käyttäjällä on vain yksi salasana, sille voidaan kohtuudella asettaa suurempia laatuvaatimuksia ja tiheämpi vaihtoväli.

Jos käyttäjällä on vain yksi käyttäjätunnus ja salasana, niin onko silloin kaikki munat samassa korissa? Yhden paljastuneen salasanan avulla voidaan toki väärinkäyttää montaa eri palvelua. Toisaalta jos käyttäjällä on yksi keskitetysti ylläpidetty identiteetti, on saatu luotua edellytyksiä **syRJäYttää salasana-tunnistus vahvalla tunnistuksella keskitetysti**. Kun käyttäjällä on tietojärjestelmissä yksi identiteetti, voidaan keskitettyyn identiteettiin liittää vahvan tunnistuksen välineitä. Näin vahvan tunnistuksen käyttöönotto keskitettyyn identiteettiin nojaavissa tietojärjestelmissä helpottuu, ja vahvan tunnistuksen välineisiin tehtävä panostus saadaan hyödynnettyä mahdollisimman laajasti.

Keskitetty näkymä käyttäjän tietoihin ja käyttövaltuuksiin **helpottaa jäljitettävyyttä ja raportointia**. Organisaation tietoturvapäällikkö, sisäinen tarkastaja, työntekijän esimies tai vaikkapa käyttäjä itse voi saada helpommin tutkittavakseen raportteja järjestelmän käyttäjistä, heillä olevista käyttövaltuuksista ja siitä, miten valtuuksia on käytetty.

## 2.2. Tehokkuus

Rationaalisesti toimiva organisaatio pyrkii tehostamaan toimintaansa karsimalla tai automatisoimalla työläitä käsin tehtäviä rutiineja. Organisaation työntekijöille tehokkuus näkyy työajan säästönä ja asioiden nopeampina läpimenoaikoina, organisaation asiakkaat puolestaan pääsevät nauttimaan nopeammasta ja paremmasta palvelusta.

Jos loppukäyttäjällä on vain yksi tai pieni määrä käyttäjätunnus/salasana-pareja, joita hän vastaavasti joutuu käyttämään useammin, hänen edellytyksensä oppia salasana ulkoa kasvaa. Näin **unohtuneiden salasanojen muisteluun ja etsimiseen menevä työaika vähenee**. Jos käyttäjä joutuu pyytämään IT-tuesta uutta salasanaa, hän **aiheuttaa työkuormaa myös IT-palvelupisteeseen**. Huomattava määrä organisaatioiden IT-palvelupisteisiin tulevista tukipyynnöistä koskee unohtuneiden salasanojen resetoimista.

On todennäköistä, että samat henkilöt käyttävät organisaation eri tietojärjestelmiä. Jos jokaisessa tietojärjestelmässä on oma käyttäjätunnustietokantansa, käyttäjätilien perustamisessa, ylläpidossa ja sulkemisessa tehdään paljon moninkertaista ja päällekkäistä työtä. Lisäksi käyttäjätietojen eheys on uhattuna; kun käyttäjän tiedot muuttuvat, muutos muistetaan ehkä viedä vain osaan järjestelmistä, ja lopulta käyttäjätietokannoissa on myös paljon keskenään ristiriitaista tietoa. **Käyttäjien identiteettien keskitetty hallinta karsii samojen tietojen moninkertaista ylläpitämistä ja lisää tiedon laatua**. Tarkoituksenmukaisilla välineillä myös käyttäjätunnus- ja käyttövaltuushakemusten läpimenoaikaa saadaan nopeutettua.

Identiteetinhallinnan keskittäminen organisaatiossa tuo usein myös **tavanomaisia suuruuden ekonomiaan liittyviä hyötyjä**. Yhteen paikkaan keskitettynä samoilla resursseilla voidaan saada aikaan enemmän; käyttöön voidaan ottaa esimerkiksi kehittyneempiä välineitä ja identiteetinhallintaa operoiville työntekijöille toteuttaa varamiesjärjestelyjä.

### 2.3. Uudet toimintatavat

Tietoturvallisuuden kasvun ja toiminnan tehostumisen lisäksi identiteetin- ja pääsynhallinnan kehittäminen saattaa avata myös mahdollisuuksia järjestää organisaation toimintaa uudelleen tai kehittää uusia liiketoimintamalleja. Avautuvat mahdollisuudet riippuvat organisaation toimintaympäristöstä.

Identiteetin- ja pääsynhallinnan keskittäminen organisaatiossa esimerkiksi sisäiseen tietohallintoon mahdollistaa muiden yksiköiden vapautumisen ainakin osaksi identiteetin- ja pääsynhallinnan tehtävistä. Käyttäjätunnus- ja käyttövaltuusylläpidosta vapautunut aika voidaan kohdentaa yksikössä sen ydintoimintaan, joka useinkaan ei ole käyttäjätunnusylläpito.

Esimerkiksi nykyään organisaation työntekijät tekevät matkalaskunsa yleensä siihen tarkoitetulla matkahallintajärjestelmällä, johon työntekijät, matkalaskun hyväksyjät, reskontranhoitajat ja muut matkalaskuihin liittyvät henkilöt kirjautuvat henkilökohtaisella käyttäjätunnuksellaan. Matkahallintajärjestelmän omistaa esimerkiksi organisaation taloushallintoyksikkö, joka luo ja toimittaa työntekijöille siihen tarvittavan käyttäjätunnuksen ja salasanan ja antaa heille organisaation toimintakäytäntöjen mukaiset käyttövaltuudet. Jos matkahallintajärjestelmä kuitenkin saadaan nojaamaan organisaation tietohallinnon ylläpitämiin käyttäjätunnuksiin, salasanoihin ja jopa käyttövaltuuksiin, vapautuu taloushallinnon työntekijöiden työaika käyttäjätunnusylläpidosta sellaisiin tehtäviin, jotka varsinaisesti edellyttävät taloushallinnon ammattitaitoa.

Tietotekniikan käytön laajeneminen on luonut suuntauksen, jossa itsepalvelut ja sitä tukevat tietojärjestelmät lisääntyvät organisaatioissa. Jos aikaisemmin työntekijä on hoitanut esimerkiksi kehityskeskustelun, matkalaskun teon tai ostolaskun hyväksymisen lähettämällä paperisia dokumentteja talous- tai henkilöstöhallintoyksikköön, on nykyään tavallista että käyttäjä kirjautuu asiaan liittyvään sähköiseen palveluun omilla käyttäjätunnuksillaan. Jos kirjautumiseen tarvittava käyttäjätunnus ja salasana ovat palvelusta riippumatta samat, voidaan itsepalveluperiaate ottaa käyttöön myös niissä palveluissa, joita tavallinen työntekijä käyttää harvoin. Jos sen sijaan puolivuositain käytävä kehityskeskustelu edellyttäisi erillisen käyttäjätunnuksen ja salasanan muistamista, olisivat useimmat sen jo unohtaneet.

Toinen suuntaus organisaatioiden tietohallinnossa on tietojärjestelmien ulkoistaminen esimerkiksi pilvipalveluun (Software as a Service, SaaS), joissa organisaatio ostaa tietojärjestelmää palveluna sen ylläpitoon erikoistuneelta yritykseltä. Identiteetin- ja pääsynhallinnan avulla voidaan toteuttaa järjestely, jossa myös vuokrasovelluksiin kirjaudutaan samalla käyttäjätunnuksella ja salasalla kuin organisaation omiin palveluihin.

### 2.4. Haasteita

Kuten kehitysprojekteissa yleensä, myös identiteetin- ja pääsynhallinnan kehittämisessä on haasteita, jotka kehittäjän täytyy tunnistaa ja voittaa. Haasteet eivät useinkaan ole luonteeltaan teknisiä.

Koska norsuakaan ei voi syödä kerralla, on organisaation identiteetin- ja pääsynhallinnan kehittämisen **painopisteiden asettaminen ja priorisoiminen** välttämätöntä. Halutaanko kertakirjautumista, vai onko vahva autentikointi tärkeää? Lähdetäänkö ensiksi hakemaan säästöjä karsimalla käyttäjätietojen päällekkäistä ylläpitotyötä? Onko tärkeää helpottaa käyttövaltuuksien hakemista ja nopeuttaa hakemusten läpimenoaika? Toimiiko

organisaatio toimialalla, jossa jäljitettävyys ja raportointi on erityisen tärkeää, ja tilintarkastajat ovat osoittaneet niissä puutteita? Kehittämisen painopisteiden asettaminen edellyttää näkemystä organisaation toiminnasta ja tietoturvapäämääristä. Dilemma tässäkin projektissa on, että projektin painopisteet joudutaan asettamaan jo alkuvaiheessa, jolloin projektin vastuuhenkilöiden omat kokemukset ovat vähäisimmät.

Kun projektin vastuuhenkilöt ovat muodostaneet kuvan identiteetin- ja pääsynhallinnan kehittämiskohteista, heidän pitäisi pystyä käymään keskustelua ja **perustelemaan johdolle, miksi identiteetin- ja pääsynhallinnan projektiin pitäisi osoittaa resursseja.** IT-projektit voivat olla johdolle vaikeita ymmärtää, ja IT-projektien joukossa identiteetin- ja pääsynhallinnan projektit eivät useinkaan ole kaikkein helpoimmin ymmärrettäviä. Projektin lopputulos ei välttämättä ole yksittäinen konkreettinen palvelu, joka helposti nähtävällä tavalla auttaisi organisaatiota saavuttamaan päämääränsä.

Kun projekti on saanut käynnistyslupan, kohdataan kenties suurin haaste, joka liittyy organisaation toiminnan mallintamiseen ja määrämuotoistamiseen. Organisaatioon täytyy suunnitella ja toteuttaa **toimintakäytännöt identiteettitiedon kurinalaiseen ylläpitämiseen.** Jos käyttöön halutaan yhden käyttäjätunnuksen periaate, niin mikä organisaatioyksikkö vastaa tunnuksen luomisesta, ja minkälaisen herätteen perusteella luominen tapahtuu? Jos halutaan karsia päällekkäistä samojen käyttäjätietojen ylläpitoa, niin mikä tietovaranto korotetaan ns. master-tiedon lähteeksi, josta käyttäjätiedot kopioidaan muihin paikkoihin? Näihin kysymyksiin palataan luvussa 7.

## 2.5. Pohdittavaa

- Paraneeko vai heikkeneekö tietoturvallisuus, jos yhdellä käyttäjätunnus/salasana-parilla pääsee sisään suureen joukkoon eri palveluita?
- Kerrospuolustus on yksi tietoturvallisuuden periaate. Millä tavalla kerrospuolustusta voidaan toteuttaa identiteetin- ja pääsynhallinnassa?
- Voiko yritys saada liiketoimintaetua hyvin hoidetusta identiteetin- ja pääsynhallinnasta?
- Millä tavalla identiteetin- ja pääsynhallinnan kehitysprojektista saatavia taloudellisia hyötyjä voitaisiin arvioida ja esittää päätöksenteon tueksi?

### 3. Identiteetti

Identiteetin- ja pääsynhallinnan peruskäsitteisiin tutustuminen alkaa identiteetin käsitteestä.

#### 3.1. Käsitteitä

Tietotekniikassa (sähköinen) **identiteetti** tarkoittaa **kohdetta kuvailevien ominaisuuksien eli attribuuttien kokoelmaa**. Kohteet ovat usein ihmisiä – tietojärjestelmien käyttäjiä – joita kuvailevia attribuutteja ovat esimerkiksi nimi, käyttäjätunnus ja valtuus tietyn palvelun käyttämiseen. Käyttäjän identiteetti on tosielämän henkilön abstraktio tietojärjestelmässä – esimerkiksi käyttäjätietokannassa oleva tietue, jossa käyttäjätunnus (uid) on *eesimerk* ja jonka tiedetään kuuluvan tosielämässä tietylle Esko Esimerkki –nimiselle henkilölle.



**Kuva 2.** Identiteetti on tosielämän henkilön abstraktio tietojärjestelmässä – esimerkiksi käyttäjätietokannassa oleva tietue, jossa avainkenttänä on käyttäjätunnus *eesimerk*.

Myös muilla kohteilla kuin ihmisillä voi olla identiteetti; esimerkiksi organisaatioilla (joihin liittyviä attribuutteja ovat esim. nimi, kotipaikka ja Y-tunnus) tai verkkoon kytketyillä tietokoneilla (attribuutteina esim. IP-numero, domain-nimi ja julkinen avain). Tavallisesti identiteetin- ja pääsynhallinnan problematiikka keskittyy kuitenkin pitkälti ihmisten identiteettiin, koska organisaatioiden toiminta on kuitenkin lopulta organisaatioon liittyvien ihmisten toimintaa, ja toimiessaan organisaatiossaan tai organisaationsa nimissä ihmiset tarvitsevat monenlaisia käyttövaltuuksia erilaisiin tietojärjestelmiin. Jatkossa tämä kirja keskittyy pelkästään ihmisten identiteettien hallintaan.

On hyvä huomata, että tietotekniikan identiteetillä ei varsinaisesti ole mitään tekemistä psykologian käsitteistön kanssa, jossa identiteetillä tarkoitetaan ihmisen yksilöllistä käsitystä omasta itsestään. Väärinkäsitysten välttämiseksi tietotekniikassa voidaan puhua henkilön sähköisestä identiteetistä (digital identity), joka ei ole mitään sen ”henkisempää” kuin tietojoukko, joka on talletettu johonkin tietojärjestelmään.

Alalle on vakiintumassa käsitteistö, jonka mukaan henkilöllisyys-käsite (identity) ja (sähköinen) identiteetti -käsite (digital identity) eroavat toisistaan siten, että henkilöllä voi olla yksi henkilöllisyys mutta useita identiteettejä. Henkilöllä esimerkiksi voi olla yksi identiteetti työpaikan tietojärjestelmissä, toinen lähikaupan kanta-asiakasjärjestelmässä ja kolmas netissä olevassa sosiaalisen median palvelussa.

**Identiteetinhallinnalla (identity management, IdM) tarkoitetaan prosessia, jolla kohteet esitetään digitaalisina identiteetteinä tietojärjestelmissä.** Identiteetinhallinta on prosessi, johon liittyy tietojärjestelmien lisäksi sopimuksia identiteettitiedon syntaksista ja semantiikasta sekä toimintakäytäntöjä, joilla tietoa ylläpidetään tietojärjestelmissä ja jolla

muutokset tiedossa virtaavat tietojärjestelmien välillä. Organisaatiossa sopimusten, toimintakäytäntöjen ja tietojärjestelmien muodostama kokonaisuutta sanotaan usein organisaation identiteetinhallinta-arkkitehtuuriksi, johon palataan luvussa 7.

Identiteetinhallinta-käsitteen aisaparina käytetään usein **pääsynhallinnan (access management, AM) käsitettä, jolla tarkoitetaan sitä toimintoa, jossa tietojärjestelmän käyttäjä tunnistetaan ja tunnistuksen perusteella päätetään, onko käyttäjällä pääsy tietojärjestelmään**. Siinä missä identiteetinhallinta tarkoittaa käyttäjän kannalta usein näkymättömissä tapahtuvaa käyttäjätiedon hallintaa ja virtaamista ”taustajärjestelmien” välillä, pääsynhallinta tarkoittaa käyttäjälle näkyvää tapahtumasarjaa, jossa yksinkertaisimmillaan pyydetään käyttäjää antamaan käyttäjätunnuksensa ja salasansa, ja onnistuneen tunnistuksen perusteella kerrotaan, onko käyttäjällä käyttöoikeus palveluun. Yhdessä käsitteet muodostavat identiteetin- ja pääsynhallinnan yläkäsitteen (identity and access management, IAM). Pääsynhallinta esitetään usein identiteetinhallinnasta erillisenä kokonaisuutena, koska usein IAM-projektit kohdistuvat jompaankumpaan kokonaisuuteen ja yleensä IAM-tuoteperheetkin sisältävät kumpaankin omat tuotteensa. Aina ei kuitenkaan ole selvää, missä identiteetinhallinnan ja pääsynhallinnan käsitteiden välinen raja-aita kulkee.

### 3.2. Attribuutit

Identiteetti koostuu kokoelmasta attribuutteja; identiteetin voi ajatella vaikkapa palvelun käyttäjätietokannan tietueeksi, jossa jokainen attribuutti on yksi tietokannan sarake. Käyttötilanteesta riippuu, mitä attribuutteja identiteettiin kulloinkin tarvitsee liittää; itse asiassa muiden kuin tarpeellisten attribuuttien kerääminen ja tallettaminen henkilöstä kielletään henkilötietolaissa (luku 9). Määritystä käyttäjätietokantaan kerätyistä attribuuteista kutsutaan käyttäjätietokannan skeemaksi.

Palvelun kehittäjä voi toki rakentaa skeemansa alusta lähtien itse, mutta identiteetinhallintatuotteiden skeemat nojaavat usein Internet-standardeina julkaistuihin olioluokkiin (object class). Ne on alkujaan kehitetty LDAP-hakemistoja (luku 7.6) ja sen edeltäjiä varten, mutta joita käytetään identiteetinhallintatuotteissa myös laajemmin. Alla olevaan taulukkoon on koottu joitain attribuutteja esimerkiksi.

Attribuutti	Selitys	Lähde
Cn	Koko nimi	RFC 4519
Sn	Sukunimi	RFC 4519
Mail	Sähköpostiosoite	RFC 2798
telephoneNumber	Puhelinnumero	RFC 4519
Uid	Käyttäjätunnus	
Password	Salasana (tiivisteinä)	
employeeNumber	Työntekijänumero	RFC 2798
preferredLanguage	Toivottu asiointikieli	RFC 2798
eduPersonAffiliation	Henkilön rooli	eduPerson

	korkeakoulussa, esim. student, staff, faculty	
--	--	--

### 3.3. Yksilöivät tunnisteet

Käyttäjän attribuuttien joukossa erityistarkastelun ansaitsevat yksilöivät tunnisteet (unique identifier), joiden tehtävä on erottaa käyttäjät vertaisistaan jossain nimiavaruudessa. Allaolevaan taulukkoon on koottu joitain tyypillisiä yksilöiviä tunnisteita.

Yksilöivä tunniste	Nimiavaruus
Käyttäjätunnus	Tietojärjestelmä tai useita tietojärjestelmiä, jos organisaatiossa on käytössä keskitetty identiteetinhallintajärjestelmä
Sähköpostiosoite	Internetin SMTP-pohjainen sähköpostipalvelu
Henkilötunnus (Suomessa)	Väestötietojärjestelmä; Suomen kansalaiset tai Suomessa pysyvästi tai pitkäaikaisesti oleskelevat ulkomaalaiset.
Työntekijänumero	Työnantaja, työnantajan henkilöstöhallinnon järjestelmät
Opiskelijanumero	Oppilaitos
Skype name	Käyttäjän yksilöivä tunniste Skypen internet-puhelupalvelussa
Passin numero	Passin myöntänyt valtio

Nimiavaruudella tarkoitetaan sitä joukkoa, jossa yksilöivä tunniste on yksikäsitteinen. Esimerkiksi Tampereen teknillisen yliopiston identiteetinhallintajärjestelmässä käyttäjätunnus *linden* tiedetään varmasti kuuluvan täsmälleen yhdelle<sup>1</sup> henkilölle kerrallaan. Mikään ei kuitenkaan estä Aalto-yliopistoa antamasta samaa käyttäjätunnusta omassa identiteetinhallintajärjestelmässään aivan eri henkilölle.

Paikallisesti hallittuja nimiavaruuksia voidaan kuitenkin yhdistellä nimiavaruuksien **hierarkian**, esimerkiksi Internetin DNS-järjestelmän, avulla. Niinpä voidaan ottaa käyttöön esimerkiksi tunnisteet [linden@tut.fi](mailto:linden@tut.fi) ja [linden@aalto.fi](mailto:linden@aalto.fi), jotka yleensä viittaavat eri henkilöihin. Hierarkinen nimiavaruus on käytössä esimerkiksi Internetin SMTP-sähköpostijärjestelmässä tai maa- ja suuntanumeroita sisältävissä puhelinnumeroissa.

Yksilöivät tunnisteet ovat keskeisessä asemassa identiteetinhallinnan arkkitehtuurissa, koska niiden avulla voidaan yksikäsitteisesti viitata tiettyyn käyttäjään. Toisaalta niihin liittyy myös joitain keskeisiä piirteitä, joihin tarvitsee ottaa kantaa organisaation identiteetinhallinta-arkkitehtuurissa:

- **Kattavuus.** Määritelmänsä mukaan yksilöivä tunniste pitää voida antaa jokaiselle identiteetinhallintajärjestelmän piirissä olevalle henkilölle – se arvoa ei siis voida jättää

<sup>1</sup> Yleensä käyttäjä on käyttäjätunnuksen saadessaan sitoutettu käytösääntöihin, joissa häntä kielletään jakamasta käyttäjätunnusta (ja sen salasanaa) kenenkään kanssa. Oma lukunsa on ryhmätunnukset, joiden salasana on kaikkien ryhmän jäsenten tiedossa. Ryhmätunnuksia pyritään välttämään jäljitettävyyssyistä. Jäljitettävyyteen palataan luvussa 6.1.



kenellekään tyhjäksi. Yksilöivä tunniste täytyy siis valita siten, että kaikilla nykyisillä ja tulevilla käyttäjillä on tai heille voidaan järjestää arvo yksilöivälle tunnisteelle.

Jos yksilöivänä tunnisteena käytetään henkilötunnusta, niin kuinka menetellään esimerkiksi ulkomaalaisen henkilön kohdalla, jolla sitä ei ole? Jos henkilökunnan yksilöivänä tunnisteena esimerkiksi käytetään henkilöstöhallinnon antamaa työntekijänumeroa, niin onko mahdollista, että identiteetinhallinnan piiriin joskus tulee henkilöitä joita ei viedä henkilöstöhallinnon järjestelmiin eikä henkilökuntanumeroa siten ole (esimerkiksi konsultteja, jotka eivät ole työsuhteessa organisaatioon, vaan sen alihankkijaan).

- **Lukumääräsuhteet eli kardinaliteetit.** Voiko samalla henkilöllä olla useita rinnakkaisia yksilöivän tunnisteiden arvoja? Esimerkiksi edellä taulukossa passin numero on attribuutti, joita samaan henkilöön liittyy useita – ainakin sitten kun passi vanhenee ja hän hankkii uuden. Onko käyttäjällä identiteetinhallintajärjestelmässä aina täsmälleen yksi käyttäjätunnus? Onko työntekijällä täsmälleen yksi työntekijänumero, vaikka hänellä olisi organisaatioon useita rinnakkaisia tai perättäisiä palvelussuhteita? Onko yliopisto-opiskelijalla yksi ja sama opiskelijanumero, vaikka hän olisi ensin opiskellut avoimessa yliopistossa ja sen jälkeen aloittanut tutkinto-opiskelijana? Jos henkilö on oppilaitoksessa sekä opiskelija että työntekijä, niin onko hänellä yksi vai kaksi käyttäjätunnusta? Pystyykö pankin tietojärjestelmä tunnistamaan tilanteen, jossa sama henkilö on sekä pankin työntekijä että pankin asiakas?
  - **Revokointi** (revocation). Voiko kytkös tietyn henkilön ja yksilöivän tunnisteiden väliltä katketa; toisin sanoen: voiko tietty yksilöivä tunniste lakata viittaamasta tiettyyn henkilöön. Usein tämä liittyy kysymykseen: voiko henkilön yksilöivä tunniste muuttua? Esimerkiksi jos henkilön käyttäjätunnus muodostetaan hänen sukunimestään, ja sukunimi muuttuu avioliiton (tai - mikä pahempaa - avioeron) vuoksi, hän usein haluaisi, että myös hänen käyttäjätunnustaan muutetaan. Yksilöivän tunnisteiden muuttaminen on hankalaa ja virhealtista silloin, kun tunniste toimii usean tietokannan yhteisenä avainkenttänä.
- Toinen tyypillinen esimerkki liittyy sähköpostiosoitteeseen: tämän kirjan kirjoittaja on käyttänyt [mikael.linden@tut.fi](mailto:mikael.linden@tut.fi) –sähköpostiosoitettaan jo kolmella vuosikymmenellä. Jos syksyllä työt Tampereen teknillisessä yliopistossa sattuu aloittamaan samanniminen työntekijä, niin saako kirjoittaja pitää sähköpostiosoitteensa, vai annetaanko sekaannuksien välttämiseksi molemmille [mikael.x.linden@tut.fi](mailto:mikael.x.linden@tut.fi) –tyyppinen sähköpostiosoite, jossa x on esimerkiksi omistajansa toisen nimen ensimmäinen kirjain?
- **Kierrätys** (re-assignment). Jos yksilöivä tunniste vapautuu, niin voidaanko vapautunut tunniste myöhemmin antaa toiselle henkilölle. Esimerkiksi, jos [mikael.linden@tut.fi](mailto:mikael.linden@tut.fi) –sähköpostiosoite vapautuu, niin voiko seuraavana syksynä työt aloittava samanniminen henkilö saada vapautuneen sähköpostiosoitteen, vai jäädytetäänkö se ikuisesti (tai ainakin siihen saakka, kun sen alkuperäinen omistaja palaa organisaatioon ja saa sen takaisin).

Jäljitettävyyksivaatimukset saattavat asettaa vaatimuksia yksilöivän tunnisteiden kierrätyskäytännöille; vielä pitkänkin ajan jälkeen saattaa olla tarve näyttää (ääritapauksessa tuomioistuimessa), kenelle tietty käyttäjätunnus on jonkun tapahtuman tekohtekellä kuulunut. Siinä missä yksilöivän tunnisteiden revokointimahdollisuus siis

vaikuttaa koettuun käyttömukavuuteen, tunnisteiden kierrättäminen vaikuttaa järjestelmän tietoturvaluuteen. Jäljitettävyyteen palataan luvussa 6.

Yksilöivää tunnistetta rakennettaessa tehtävä merkittävä valinta on tunnisteiden syntaksiin mahdollisesti sisällytettävä semantiikka. Jos tunnisteeseen sisällytetään semantiikkaa, sitä useammin kohdataan tilanteita, joissa syntyy tarve muuttaa tunnisteiden arvoa (revokointi) tai tunnisteiden huomataan alkaneen nakertamaan haltijansa yksityisyyttä. Siksi yksilöivän tunnisteiden semantiikkaa valittaessa on tarpeen punnita tarkkaan tehtäviä valintoja ja niiden seurauksia. Esimerkiksi

- Jos käyttäjätunnus sisältää henkilön **sukunimen** ja sukunimi muuttuu, haluaisivat monet käyttäjät myös, että hänen käyttäjätunnustaan muutetaan.
- Jos käyttäjätunnus sisältää tiedon **organisaatioyksiköstä**, johon työntekijä kuuluu, aiheuttaa organisaatiorakenteen uudistaminen tai henkilöiden siirtyminen organisaatioyksiköstä toiseen paineen muuttaa käyttäjätunnuksia.
- Taannoin matkapuhelinnumeron alun ”**suuntanumero**” kertoi, minkä teleoperaattorin liittymästä oli kyse. Jos henkilö vaihtoi puhelinliittymää, myös hänen puhelinnumeronsa vaihtui, mikä vaikeutti telemarkkinoiden vapaata kilpailua. Nykyisin ”suuntanumero” ei enää yksilöi teleoperaattoria, vaan puhelinnumero voidaan säilyttää samana vaikka henkilö vaihtaisi operaattoriaan.
- Suomalaisen **henkilötunnuksen** toiseksi viimeinen merkki on naisilla parillinen ja miehillä pariton. Jos henkilö käy läpi sukupuolenkorjausleikkauksen, syntyy tarve vaihtaa hänen henkilötunnustaan. Henkilötunnuksen vaihtumisesta seuraa monenlaisia käytännön ongelmia, joita ei usein ole osattu huomioda tietojärjestelmien suunnittelussa.
- Suomalainen henkilötunnus sisältää haltijansa **syntymäajan**, ja monet pitävät ikäänsä yksityisasiana. Muun muassa tämän vuoksi henkilötunnusta pidetään jossain määrin arkaluontoisena henkilötietona. Sähköisessä asiointissa Väestörekisterikeskus onkin alkanut tuomaan sen rinnalle sähköistä asiointitunnusta (satu), joka on juokseva, vailla mitään semantiikkaa oleva numero.

### 3.4. Pseudonyymit eli salanimet

Identiteettiä kuvattiin edellä tosielämän henkilön abstraktioksi tietojärjestelmässä. Usein asiaan kuuluu, että tietojärjestelmän ylläpitäjä tai muut käyttäjät tietävät, ketä tosielämän henkilöä tietty identiteetti edustaa. On kuitenkin käyttötilanteita, joissa vastaavan tosielämän henkilön tietäminen ei ole mielenkiintoista tai se halutaan nimenomaan välttää. Tällöin kysymys on pseudonymistista identiteetistä ja yksilöivä tunniste on pseudonyymi tunniste (pseudonymous identifier) eli salanimi.

Pseudonymia identiteettiä voi käyttää esimerkiksi keskustelupalstoilla, jos ei halua paljastaa todellista henkilöllisyyttään. Dynaaminen IP-osoite voidaan myös ajatella henkilön pseudonymiksi tunnisteeksi, jos käytössä ei ole NAT-järjestelyä, joka kätkee saman IP-osoitteen taakse monta käyttäjää. Tällöin tosin ainakin IP-osoitteen antanut teleoperaattori pystyy selvittämään, kuka tilaaja IP-osoitteen takaa löytyy. Myös WWW-selainten käyttämä eväste (cookie) voidaan ajatella pseudonymiksi tunnisteeksi; se ei välttämättä paljasta WWW-palvelimelle, kuka tosielämän käyttäjä selaimen takana istuu, mutta se kertoo kuitenkin, että käyttäjä on sama henkilö, joka selaimineen vieraili samalla WWW-palvelimella myös eilen.

### **3.5. Pohdittavaa**

- Edellä nostettiin esiin monenlaisia ongelmia, joita seuraa yksilöivään tunnisteeseen sisällytettävästä semantiikasta. Miksi yksilöivät tunnisteet kuitenkin mielellään valitaan niin, että niihin sisällytetään semantiikkaa?
- Minkälaisia ongelmia organisaatiolle saattaa syntyä siitä, että samalla henkilöllä on organisaatiossa useita identiteettejä? Entä henkilölle itselleen? Voiko monesta identiteetistä olla peräti jotain hyötyä?

## 4. Identiteetin todentaminen eli autentikointi

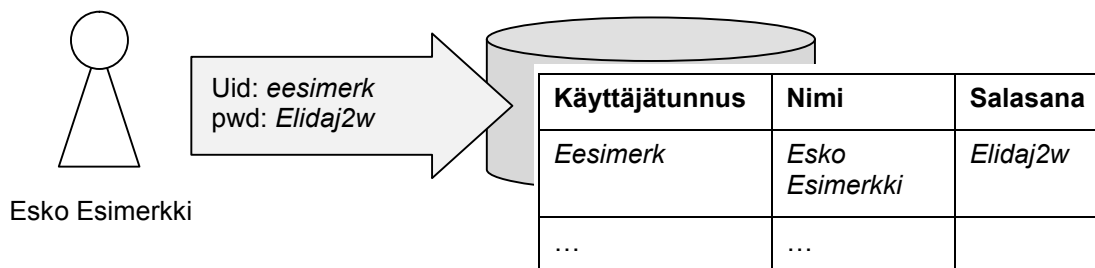
Edellisessä luvussa identiteetti määriteltiin attribuuttien joukoksi, joka edustaa tiettyä tosielämän henkilöä tietojärjestelmässä. Tässä luvussa syvennyttään identiteetin todentamiseen (verification of the identity) eli autentikointiin (authentication), josta suomen kielessä yleensä käytetään termiä käyttäjän tunnistaminen<sup>2</sup>.

Tässä luvussa tutustutaan ensin autentikoinnin käsitteeseen sekä autentikoinnin luotettavuuden eli vahvuuden arvioimiseen ja sitä koskeviin viitekehyksiin. Kertakirjautumista käsitellään lyhyesti. Lopuksi tutustutaan tarkemmin muutamiin identiteetin todentamiseen käytettyihin menetelmiin.

### 4.1. Autentikoinnin määritelmä ja menetelmät

Identiteetin todentaminen tarkoittaa, että **identiteetin ja sitä tosielämässä vastaavan henkilön välille rakennetaan kytkös**: tavalla tai toisella tietojärjestelmä varmistaa, että järjestelmään kirjautuu sisään juuri sama henkilö, jolle tietty järjestelmään luotu identiteetti kuuluu. Autentikointia ei siis voida ajatella tehtävän ilman, että käyttäjällä on järjestelmässä ainakin jonkinlainen identiteetti.

Kytös on yleensä voimassa istunnon (session) ajan, ja istunto suojataan tavallisesti kryptografisesti, kuten symmetrisellä istuntoavaimella. Istunto päättyy, kun käyttäjä kirjautuu ulos (logout).



**Kuva 3. Kun identiteetti todennetaan, tietojärjestelmä varmistaa esimerkiksi salasanalla, että järjestelmään kirjautuu sisään juuri sama henkilö, jolle tietty järjestelmään luotu identiteetti kuuluu.**

Identiteetin todentamiseen on lukuisia erilaisia, luotettavuudeltaan vaihtelevia menetelmiä ja välineitä, jotka yleensä jaetaan kolmeen ryhmään:

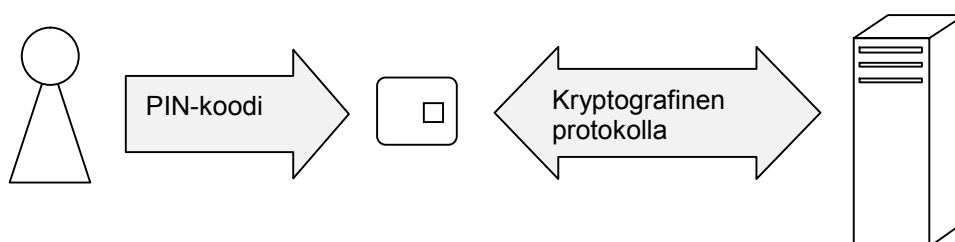
1. **Jotain, mitä henkilö tietää tai muistaa**, kuten salasana tai PIN-koodi. Salasanat ovat edelleen vallitseva tunnistustapa, vaikka niihin liittyvät ongelmat tunnetaan: salasana voidaan kurkkia olan yli tai kaapata sen kulkiessa päätelaitteen kautta autentikoivalle palvelimelle, se on altis välimieshyökkäyksille (mm. kalastelu eli phishing) ja huoleton käyttäjä kirjoittaa sen ylös muistinsa tueksi. Jos käyttäjällä on vapaus valita salasanansa itse, hänellä on taipumus valita helposti arvattava salasana, ja käyttää samaa salasanaa

<sup>2</sup> Toisinaan Suomen kielen käsitteiden tunnistaminen ja todentaminen erona pidetään sitä, että käyttäjä tunnistetaan, kun hän esittää väitteen identiteetistään (esimerkiksi antaa käyttäjätunnuksensa) ja tunnistaminen todennetaan, kun väitteen todenperäisyys tarkistetaan (esimerkiksi käyttäjä antaa salasanansa). Laki vahvasta sähköisestä tunnistamisesta kuitenkin kutsuu tunnistamiseksi kokonaisuutta, joka sisältää nämä molemmat kohdat.

useassa eri palvelussa. Salasanatunnistuksen hyvä puoli on sen helppo ja edullinen käyttöönotto ja konseptin tuttuus loppukäyttäjille.

2. **Jotain, mitä henkilöllä on hallussaan**, kuten toimikortti (smart card), toimiavain (token), pankkikortti, matkapuhelin, kertakäyttösalasanalista tai niitä generoiva laite. Tunnistuksesta on mahdollista tehdä salasanatunnistusta luotettavampi, mutta fyysisen tunnistusvälineiden jakeluun liittyvä logistiikka aiheuttaa lisävaivaa ja –kustannuksia. Jos tunnistusväline on päätelaitteeseen kytkettävä lisälaite, pitää käytetyn päätelaitteen laitteiston ja ohjelmiston pystyä tukemaan sitä. Esimerkiksi toimikortin käyttäminen edellyttää päätelaitteelta toimikortinlukijaa ja siihen liittyvää ohjelmistoa.
3. **Jotain, mitä henkilö on tai kuinka hän käyttäytyy, eli biometrinen tunnistus**. Biometrinen tunnistus perustuu johonkin henkilön yksilölliseen ominaisuuteen, kuten sormenjälkeen, kädenmuotoon, kasvojen muotoon, silmän iiriksen kuvioihin tai tapaan, jolla henkilö tekee allekirjoituksen tai naputtelee näppäimistöä. Biometrisen tunnistuksen hyvä puoli on, että tunnistusväline kulkee automaattisesti haltijansa mukana eikä sitä voi hukata, unohtaa tai lainata. Biometriseen tunnistukseen palataan luvussa 4.6.

Usein autentikointia pidetään vahvana (strong authentication), jos vähintään kaksi turvatekijää eri ryhmistä on yhtä aikaa läsnä (multifactor authentication, MFA). Esimerkiksi pankkiautomaatin käyttämiseen tarvitaan sekä kortti että PIN-koodi, samoin toimikortin käyttämiseen. Verkkopankkien kirjautuminen Suomessa edellyttää sekä salasanaa että kertakäyttösalasanaa. Vahvan tunnistamisen vastakohta on heikko eli kevyt tunnistaminen.

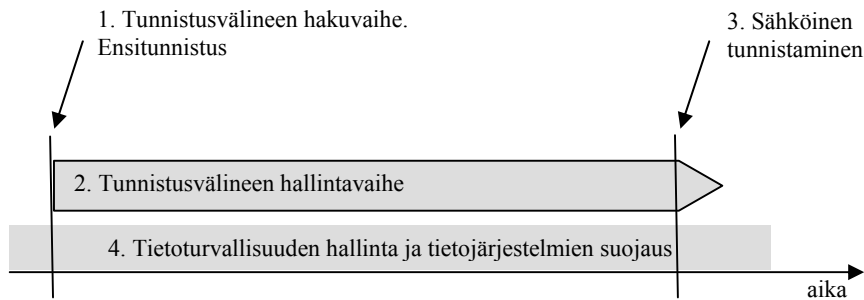


**Kuva 4. Esimerkki heikon ja kryptografisen tunnistuksen yhteispelistä; toimikortti tunnistaa käyttäjän heikosti salasanalla ja palvelin tunnistaa toimikortin kryptografisella protokollalla.**

Koneet voivat lisäksi tunnistaa toisensa kryptografisella protokollalla, joka perustuu symmetriseen tai epäsymmetriseen avainpariin. Koska kryptografiassa käytettävät laskutoimitukset ovat monimutkaisia ja salausavaimet pitkiä, ei kryptografista protokollaa voi ajatella käytettävän ihmisen tunnistamiseen. Kryptografialla on kuitenkin usein osuutensa myös käyttäjän tunnistuksessa (Kuva 4); esimerkiksi toimikortilla tapahtuvassa käyttäjän tunnistuksessa toimikortti tunnistaa käyttäjän PIN-koodilla, ja palvelin toimikortin kryptografisella protokollalla. Julkisen avaimen järjestelmään ja toimikortteihin palataan luvussa 4.4.

## 4.2. Ensitunnistus ja tunnistuksen luotettavuus

Edellisessä alaluvussa käsiteltiin sitä kirjautumishetkellä tapahtuvaa, kenties muutaman sekunnin kestävästä tapahtumasarjasta, jonka tuloksena tietojärjestelmä todensi käyttäjän identiteetin. Usein se ei yksin kuitenkaan riitä luotettavan käyttäjätunnistuspalvelun toteuttamiseen, vaan huomiota joudutaan kiinnittämään myös siihen laajempaan kokonaisuuteen, jolla tunnistusvälineitä luodaan ja hallinnoidaan tunnistuspalvelussa.



**Kuva 5. Tunnistuksen luotettavuuden osatekijät.**

Tunnistuksen luotettavuutta arvioitaessa huomiota kiinnitetään seuraaviin neljään osatekijään (Kuva 5). Tunnistuksen vahvuutta koskevat standardit ja viitekehykset asettavat kullekin osatekijälle vaatimuksia, jotka ovat sitä korkeampia, mitä luotettavampaa tunnistusta tavoitellaan:

1. **Tunnistusvälineen hakuvaihe.** Hakija hakee tunnistusvälinettä ja hänelle kerrotaan tunnistuspalvelun käyttöehdot. Hakija **ensitunnistetaan** (identity proofing) eli hänen henkilöllisyytensä todennetaan tunnistuksen vahvuustason edellyttämällä tavalla. Tunnistusvälineen hakuvaiheesta syntyvät dokumentit arkistoidaan myöhempää näyttöä varten.
2. **Tunnistusvälineen hallintavaihe.** Tunnistusväline luodaan ja sen tiedot yhdistetään haltijaansa. Tunnistusväline toimitetaan haltijalleen tunnistuksen vahvuustason edellyttämällä tavalla ja aktivoidaan esimerkiksi eri kanavaa toimitetulla aktivointikoodilla, jos tarpeen. Tunnistusvälineen haltija huolehtii välineen säilyttämisestä turvallisesti. Tarvittaessa tunnistusväline voidaan peruuttaa väliaikaisesti (suspension) tai pysyvästi (revocation). Voimassaolon päättyessä voimassaoloa voidaan jatkaa (renewal) tai tunnistusvälineen tilalle toimittaa uusi väline (replacement). Tunnistusvälineen hallintavaiheen tapahtumat tallennetaan lokiin.
3. **Sähköinen tunnistaminen.** Tunnistukseen nojaava taho tunnistaa tunnistusvälineen haltijan tunnistusvälineen avulla sen mukaisesti kuin käytetty tunnistuksen vahvuustaso edellyttää. Yleensä jäljitettävyyden ja vaatimuksenmukaisuus edellyttää myös, että suoritetuista tunnistustapahtumista talletetaan tarpeelliset lokitiedot.
4. Tunnistuspalveluntarjoajan **tietoturvallisuuden hallinta ja tietojärjestelmien suojaus**, joka sisältää tavanomaisia tietoturvallisuutta tukevia kontroleja. Tunnistuspalveluntarjoajan tulee olla rekisteröitynyt oikeushenkilö, joka omaa palvelun tarjoamisen kannalta tarvittavat taloudelliset voimavarat. Tunnistuspalveluntarjoajalla tulee olla tarpeelliset tietoturvallisuuden ja riskien hallinnan suunnitelmat, toimintakäytännöt ja kontrollit, jotka auditoidaan tunnistuksen vahvuustason edellyttämällä tavalla.

Lisätietoa: ITU-T X.1254 ja ISO/IEC 29115.

Usein tunnistuksen luotettavuutta arvioitaessa tarkastelu pelkistetään kahteen tekijään: ensitunnistuksen toteutustapaan ja sähköisen tunnistuksen toteutustapaan. Kuva 6 havainnollistaa näistä syntyvää nelikenttää.

<b>Ensitunnistus</b> <b>Sähköinen tunnistus</b>	<b>Heikko</b> (rekisteröityminen itsepalveluna)	<b>Vahva</b> (kasvotusten)
<b>Heikko</b> (salasanalla)	Useimmat Internetin ns. ilmaiset palvelut	Monet organisaation sisäiset palvelut
<b>Vahva</b> (kahdella turvatekijällä)	Jotkut pseudonyymiä tarvitsevat palvelut	Asiointipalvelut

**Kuva 6. Heikon ja vahvan ensitunnistuksen ja sähköisen tunnistuksen muodostama nelikenttä.**

Ensitunnistusta pidetään usein vahvana, jos käyttäjä joutuu hakemaan tunnistusvälinettä henkilökohtaisesti kasvotusten esimerkiksi rekisteröintipisteestä. Tällöin hänen tulee esittää henkilöllisyydestään luotettava asiakirja, jona Suomessa on totuttu pitämään passia, poliisin myöntämää henkilöllisyystodistusta tai usein myös ajokorttia. Ensitunnistus kasvotusten on usein huomattava kustannustekijä ja logistinen haaste.

Monessa Internet-palvelussa ensitunnistus tarkoittaa käytännössä itsepalveluna tapahtuvaa rekisteröitymistä järjestelmän käyttäjäksi. Rekisteröinnissä ei sen kummemmin tarkisteta syötettyjen henkilötietojen paikkansapitävyyttä pois lukien ehkä sähköpostiosoite, joka voidaan tarkistaa yksinkertaisella kättelyprotokollalla: osoitteeseen lähetetään viesti, jonka avulla käyttäjä voi saattaa rekisteröitymisen loppuun. Tällöin kysymys on heikosta ensitunnistuksesta ja käytännössä pseudonyymistä identiteetistä (luku 3.4).

Usein palvelut asettuvat nelikentässä diagonaalille: heikosti ensitunnistettut käyttäjät kirjautuvat palveluun salasanalla, tai sitten (usein julkishallinnon) asiointipalvelut edellyttävät sekä vahvaa ensitunnistusta että vahvaa sähköistä tunnistusta. Siksi monet (seuraavassa alaluvussa esiteltävät) tunnistuksen luotettavuutta kuvaavat viitekehukset ilmaisevatkin tunnistuksen vahvuutta yksiulotteisella arvolla: kun siirrytään korkeammalle luotettavuustasolle, sekä ensitunnistuksen että sähköisen tunnistuksen luotettavuus kasvaa.

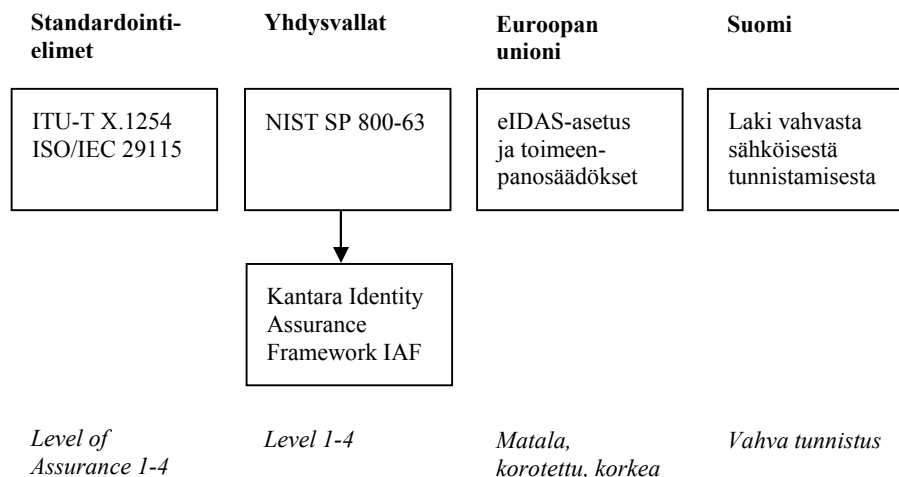
On kuitenkin hyvä huomata, että on myös käyttötilanteita (nelikentän vasen alakulma), joissa palvelu ei ole lainkaan kiinnostunut käyttäjän todellisesta henkilöllisyydestä, mutta tarjoaa kuitenkin vahvan sähköisen tunnistamisen, koska heikon autentikoinnin pettämisen on havaittu aiheuttavan ongelmia loppukäyttäjille ja palveluntarjoajalle. Toisaalta, vaikka monessa organisaatiossa ei olekaan otettu käyttöön henkilökunnan vahvaa sähköistä tunnistusta, on ensitunnistus toteutettu kuitenkin tyypillisesti vahvasti (nelikentän oikea yläkulma): työntekijän henkilöllisyys todennetaan ja hän saa käyttäjätunnuksensa ja salasanansa henkilökohtaisesti palvelussuhteensa alussa.

Yhteiskunnallisessa keskustelussa on noussut esiin identiteettivarkauden käsite, joka on kriminalisoitu syyskuusta 2015 alkaen. Vaikka myös olemassa olevan identiteetin pystyy kaappaamaan vaikkapa salasanan arvaamalla, identiteettivarkaus perustuu usein kuitenkin juuri palveluiden heikkoon ensitunnistukseen. Kuka vain voi rekisteröityä palveluun jonkun muun henkilötiedoilla, ja varsinkin uhrin henkilötunnuksen tietäminen avaa mahdollisuuksia identiteetin väärinkäyttöön. Riittävän pitkään toimittuaan identiteettivaras voi saada verkossa myös uskottavuutta henkilönä, joka hän ei ole.

Lisätietoa: Rikoslaki, 38 luku, 9a§

### 4.3. Tunnistuksen vahvuuden standardeja ja viitekehyksiä

Tarve yhteismitallistaa ja vertailla erilaisten tunnistuspalveluiden luotettavuutta on synnyttänyt standardeja ja muita viitekehyksiä, joissa tunnistuksen vahvuutta on jaettu osatekijöihin ja osatekijöille on laadittu mitattavissa olevaa metriikkaa. Alla esitetään lyhyesti näistä joitain keskeisimpiä.



**Kuva 7. Tunnistuksen vahvuuden (Level of Assurance) standardeja ja muita viitekehyksiä. Määrittelyssä esitetyt tunnistuksen vahvuustasot kursivoilla.**

**NIST SP 800-63** on vanhin ja tunnetuin tunnistuksen vahvuuden määrittely, josta muut määrittelyt ovat saaneet vaikutteita. SP 800-63 määrittelee neljä turvatasoa (Level 1-4), joista Level 1 on heikoin ja Level 4 vahvin. Koska SP 800-63 on vielä melko abstrakti, Kantara-niminen teollisuusvetoinen yhteenliittymä on syventänyt sen **Identity Assurance Framework** -nimiseksi kehikoksi. Kantara IAF pyrkii olemaan riittävän yksityiskohtainen, jotta sitä vastaan voidaan suorittaa tunnistuspalvelun ulkoinen auditointi.

Euroopan unionin **eIDAS-asetus** (910/2014) rakentaa edellytyksiä jäsenvaltioiden rajat ylittävälle sähköiselle kirjautumiselle. Asetus velvoittaa jäsenmaiden julkishallinnon verkkopalvelut hyväksymään myös muissa jäsenmaissa myönnettyt tunnistusvälineet syyskuusta 2018 alkaen. Asetuksessa ja sitä täydentävissä toimeenpanosäädöksissä ja -ohjeissa määritellään kolme turvatasoa: matala, korotettu ja korkea, joista ensimmäisessä kyse on lähinnä heikosta tunnistamisesta.

Suomessa **laki vahvasta sähköisestä tunnistamisesta** (7.8.2009/617) määrittelee tunnistamisen vahvaksi, jos ensitunnistus on tehty henkilökohtaisesti viranomaisen myöntämästä tunnistusasiakirjasta ja sähköinen tunnistus perustuu vähintään kahteen turvatekijään (katso luku 4.1). Määritelmä vastaa likimain eIDAS:n korotettua tasoa ja liikenne- ja viestintäministeriö onkin aikeissa käynnistää lainvalmistelun kansallisen tunnistuslain yhdenmukaistamiseksi eIDAS-asetuksen kanssa.

Ainoat varsinaisen standardointielimen julkaisemat määrittelyt ovat kuitenkin ITU-T:n ja ISO/IEC:n samansisältöiset standardit **X.1254** ja **29115**, jotka määrittelevät Level of Assurance -tasot 1-4.



#### 4.4. Keinoja tukevampaan salasanatunnistukseen

Rajoituksistaan huolimatta salasanatunnistusta käytetään edelleen laajasti, eikä näytä siltä, että siitä lähitulevaisuudessa kokonaan vapauduttaisiinkaan. Salasatatunnistusta voidaan kuitenkin tukevoittaa joillakin pragmaattisilla keinoilla.

Loppukäyttäjän voi antaa itse valita salasansa, tai loppukäyttäjälle voidaan antaa järjestelmän valitsema salasana. **Järjestelmän valitsema salasana** on todennäköisesti laadukas eikä käyttäjällä voi olla samaa salasanaa missään muussa palvelussa (ainakaan vielä). Tutkimukset ovat kuitenkin osoittaneet, että jos järjestelmän valitsema salasana on valittu täysin satunnaisesti, käyttäjä joutuu todennäköisesti kirjoittamaan sen ylös, mikä nakertaa turvallisuutta.

Jos loppukäyttäjä saa **valita salasansa itse**, hänellä on taipumus valita helposti arvattava salasana. Helposti arvattavat salasatat ovat alttiita sanakirjahyökkäyksille, joissa tarkoitusta varten kehitetty murto-ohjelma kokeilee järjestelmällisesti erilaisia yleiskielen sanoja ja niiden variaatioita. Verkon kautta tapahtuvalta sanakirjahyökkäykseltä voidaan yrittää suojautua lukitsemalla käyttäjätunnus liian monen kirjautumisyhtymisen jälkeen. Haittapuolena on tällöin altistuminen palvelunestohyökkäyksiin. Tunnus voidaan lukita myös vain määrääjäksi, mutta tämä ei suojaakaan hyvin hitailta ja pitkiltä hyökkäyksiltä (esim. yksi kokeilu tunnissa).

Käyttäjän valitsemia salasanoja voidaan tukevoittaa vaatimalla salasanoilta suurempaa **entropiaa**, eli että salasanan merkit valitaan suuremmasta merkkijoukosta (esim. pienet ja isot kirjaimet sekä numerot). Lisäksi käyttäjän valitsemaan salasanaan voidaan ajaa salasanan murto-ohjelmaa ennaltaehkäisevästi, ja näin ehkäistä liian helpon salasanan valitseminen.

Loppukäyttäjiä olisi hyvä **opastaa** riittävän pitkän ja vaikeasti arvattavan salasanan valinnassa. Laadukas salasana syntyy esimerkiksi poimimalla kirjahyllystä kirja ja valitsemalla siitä virke, jonka käyttäjä opettelee ulkoa. Salasana muodostuu virkkeen sanojen ensimmäisistä kirjaimista. Jos salasana kuitenkin unohtuu, auttaa kirjahyllyssä oleva kirja sen mieleen palauttamisessa. Salasanan alkuun voi vaikka lisätä virkkeen sivunumeron, jotta oikeaan virkkeeseen on helpompi palata.

Salasatatunnistuksen perushaavoittuvuus on alttius toistohyökkäykselle – käyttäjätunnuksen ja salasanan verkossa kaapannut henkilö voi käyttää sitä välittömästi hyväkseen. Siksi salasana on syytä lähettää palvelimelle **aina salaavan protokollan** (esim. TLS, SSH secure shell) yli. Näin päätelaitteen ja palvelimen liikennettä salakuunteleva hyökkääjä ei saa tietoonsa salasanaa. Erilaiset haittaohjelmat asiakkaan (keylogger) tai palvelimen (rootkit) päässä voivat kuitenkin päästä käsiksi salasanaan.

Hyväuskoinen käyttäjä saattaa myös antaa salasansa uskottavasti esiintyvälle soittajalle, joka vakuuttaa olevansa vaikkapa IT-tuesta (social engineering). Siksi organisaation on syytä kouluttaa käyttäjiään myös olemaan antamatta salasanaansa missään tilanteessa kenellekään toiselle. Edes IT-tuki ei tarvitse käyttäjän salasanaa tehtäviensä hoitamisessa.

Salasana antaa sijaa välimieshyökkäykselle, kun käyttäjä luulee asioivansa aidon verkkopalvelun kanssa mutta tulee tietämättään antaneeksi salasansa hyökkääjälle (kalastelu eli phishing). Välimieshyökkäys voi syntyä myös, jos käyttäjä käyttää samaa käyttäjätunnusta ja salasanaa monessa palvelussa - kuinka käyttäjä voi olla varma, että palvelimen ylläpitäjä ei ole epärehellinen ja kokeile, mitkä muutkin palvelut avautuvat käyttäjän antamalla salasalla.

Palvelun tai käyttäjän itse voi olla vaikea tietää, koska hänen salasansa on joutunut väärin käsiin. Palvelin voi etsiä kirjautumiskäyttäjymisistä anomalioita – esimerkiksi kirjautumisia poikkeuksellisista verkoista – mutta niihin liittyy riski virhetulkinnoista ja siten palvelunestosta. Tyypillisesti lisäturvaa salasanojen paljastumista vastaan haetaan kuitenkin vaatimalla salasanojen säännöllistä vaihtamista.

Tunnistuksen suorittavalla palvelimella salasana on syytä **tallettaa tiivisteenä** (hash), ei selkokiekisenä. Salasanasta saadaan tiiviste ajamalla se sopivan yksisuuntaisen funktion läpi. Näin palvelimelle murtautuva ja salasanatiedostoon lukuoikeuden saava hakkeri ei saa suoraan käyttöönsä kaikkien käyttäjien salasanoja, vaan joutuu ensin murtamaan ne esimerkiksi sanakirjakirjahyökkäyksellä.

Päällekkäisten käyttäjätunnus/salasana-parien karsiminen tukevoittaa myös salasanatunnistusta: jos käyttäjällä on muistettavanaan vähemmän salasanoja, voidaan kohtuudella olettaa, että ne ovat pidempiä, laadukkaampia, ne muistetaan ulkoa ja niitä vaihdetaan säännöllisesti. Jos salasana annetaan aina samalle tunnistuspalvelimelle, sijaa välimieshyökkäykselle jää vähemmän. Käyttäjätunnus/salasana-parien vähentämiseen palataan luvuissa 7 ja 8.

#### 4.5. Julkisen avaimen järjestelmä, varmenteet ja toimikortit

Julkisen avaimen järjestelmä (public key infrastructure, PKI) on järjestely, jota voidaan käyttää viestien salaamiseen, digitaalisen allekirjoitukseen ja muun muassa palvelinten ja käyttäjien varsin luotettavaan sähköiseen tunnistukseen verkossa. Julkisen avaimen järjestelmästä sinänsä on kirjoitettu kokonaisia kirjoja – tässä siihen syvennyttään vain sen verran kuin aihepiirin kannalta on tarpeellista.

Julkisen avaimen järjestelmä rakentuu epäsymmetrisen eli julkisen avaimen salaamenetelmän varaan: Liisa-niminen käyttäjä luo itselleen avainparin – julkisen ja yksityisen avaimen. Liisan käyttämä kryptografinen algoritmi kytkee julkisen ja yksityisen avaimen toisiinsa niin, että Liisan yksityistä avainta ei voida helposti päätellä hänen julkisen avaimensa arvosta. Yksityisen avaimensa Liisa laittaa huolellisesti talteen ja estää sen paljastumisen kenellekään muulle. Julkisen avaimen Liisa sen sijaan toimittaa kaikille niille, jotka haluavat tunnistaa hänet verkossa.

Pekka on saanut Liisan julkisen avaimen ja haluaa tunnistaa Liisan verkossa. Pekka valitsee satunnaisluvun, lähettää sen Liisalle ja pyytää häntä allekirjoittamaan sen yksityisellä avaimellaan. Liisa allekirjoittaa Pekan antaman satunnaisluvun ja palauttaa sen allekirjoitettuna Pekalle. Pekka voi nyt tarkistaa, avautuuko allekirjoitus hallussaan olevalla Liisan julkisella avaimella. Jos avautuu, tietää Pekka todella asioivansa Liisan kanssa<sup>3</sup>.

Julkinen avain yksin on vain pitkä numerojono – avain sinällään ei tiedä, kenelle se kuuluu. Liisa voi toki julkaista julkisen avaimensa sanomalehdessä tai lähettää sen tuttavapiiriinsä kuuluville henkilöille vaikkapa CD-ROM-levyllä, mutta käytännöllisempää on, että joku luotettu toimija ryhtyy varmentajaksi (certificate authority). Varmentajan tehtävä on varmistaa, kenen hallussa julkista avainta vastaava yksityinen avain on. Varmentaja myöntää julkisille avaimille varmenteita (certificate). Varmenne (Kuva 8) on

---

<sup>3</sup> Esimerkki on yksinkertaistettu, mutta jos siihen lisätään symmetrisen istuntoavaimen luominen Liisan ja Pekan välisten viestintäkanavan salaamiseen ja Pekan autentikoiminen vastaavasti Liisalle, ollaan varsin lähellä kahteen suuntaan autentikoitua TLS- tai SSH Secure Shell –protokollan kättelyä.

varmentajan digitaalisesti allekirjoittama tietojoukko, joka kytkee yhteen julkisen avaimen ja sitä vastaavan yksityisen avaimen haltijan, jota kutsutaan varmenteenhaltijaksi. Jos Liisan tuttavat luottavat varmentajaan, he voivat Liisan varmenteen avulla varmistua hänen julkisen avaimensa aitoudesta.

```
linden@hopeatili ~ $ openssl x509 -in Katainen_Jyrki_91045694V_2000287962.cer -inform der -noout -text
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 2000287962 (0x7739f8da)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=FI, ST=Finland, O=Vaestorekisterikeskus CA, OU=Organisaatiovarmenteet, CN=VRK CA for Qualified
Certificates
    Validity
      Not Before: Jul 14 07:35:31 2011 GMT
      Not After : Jul 6 21:59:59 2016 GMT
    Subject: C=FI, O=Valtioneuvoston kanslia/serialNumber=91045694V, GN=Jyrki, SN=Katainen, CN=Katainen Jyrki
91045694V
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:9d:20:66:fc:47:9e:70:f8:f8:d3:48:89:4b:9d:
          ec:30:b4:30:10:13:41:45:1b:8f:98:e5:fc:30:a6:
          64:66:5d:e0:91:21:45:73:a5:3e:fd:d2:41:ab:0a:
          36:1c:f7:b0:7c:31:01:1b:3b:5d:d3:0a:ef:7e:d0:
          54:2e:ed:b2:27:81:6d:3f:39:0a:81:41:26:14:22:
          87:36:36:e5:46:35:97:f6:43:b5:66:3c:21:e3:c9:
          a4:4d:6c:4c:80:6e:0f:6c:1e:70:7c:d5:7a:0d:c4:
          83:0f:f6:a2:d5:9f:18:73:08:ec:a4:22:98:f7:a8:
          67:9d:01:98:8b:2a:44:41:25
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints: critical
      CA:FALSE
      X509v3 Certificate Policies:
      Policy: 1.2.246.517.1.10.3.1
      User Notice:
      Explicit Text: Tutustu varmennepolitiikkaan - se certifikat policy http://www.fineid.fi/cps2
      CPS: http://www.fineid.fi/cps2/

  Authority Information Access:
    CA Issuers - URI:http://proxy.fineid.fi/ca/vrkqc.crt

  X509v3 Subject Alternative Name:
    email:jyrki.katainen@vnk.fi, othername:<unsupported>
  Netscape Cert Type:
    SSL Client, S/MIME
  X509v3 Key Usage: critical
    Digital Signature, Key Encipherment, Data Encipherment
  X509v3 Extended Key Usage:
    TLS Web Client Authentication, E-mail Protection, Microsoft Smartcardlogin
  X509v3 Authority Key Identifier:
    keyid:54:1A:02:37:8F:8E:63:DF:8F:F0:30:23:4A:A8:FC:67:57:F0:53:A8

  X509v3 CRL Distribution Points:
    URI:http://proxy.fineid.fi/crl/vrkqcc.crl

URI:ldap://ldap.fineid.fi:389/cn=%3dVRK%20CA%20for%20Qualified%20Certificates,ou=%3dOrganisaatiovarmenteet,o=%3dV
aestorekisterikeskus%20CA,dmdName%3dFINEID,c%3dFI?certificateRevocationList

  X509v3 Subject Key Identifier:
    D4:0F:16:0B:80:55:EC:7E:1C:18:AD:4B:0C:06:9F:F5:BE:98:B9:91
  Signature Algorithm: sha1WithRSAEncryption
    69:c3:f6:25:22:b0:8e:b1:fa:9c:3b:53:0a:10:e6:70:45:09:
    7b:8f:b8:69:e9:fa:16:7a:ad:60:8f:c1:43:fc:02:63:11:bc:
    0b:f1:db:71:3e:f1:bf:c3:b4:af:2c:a2:53:cb:68:96:e1:fa:
    3e:8f:5c:f8:3f:3e:77:97:e1:3c:4c:85:6b:fd:d9:2c:2c:aa:
    ed:2f:e3:c6:d2:05:80:14:c7:7b:ee:8a:2d:46:92:75:59:b4:
    ae:6c:b4:e0:64:45:ba:17:fd:58:b9:94:bc:38:3f:c7:8c:e5:
    43:2a:b2:e7:30:77:4b:df:d7:bd:a7:2f:34:f0:72:c4:64:71:
```

f6:25:35:d3:88:f5:7f:14:c3:06:d9:31:fb:6f:ba:a5:43:3d:  
31:2d:54:1b:2e:0e:33:40:08:af:92:18:99:3f:c1:4d:da:42:  
f0:5c:15:f2:84:8c:2c:a4:80:8b:d6:9e:72:f2:ab:cb:7b:ce:  
82:c8:3c:48:a4:b0:11:67:47:3a:cf:dd:f0:86:55:de:44:8f:  
07:87:0a:d4:dd:3e:9d:43:f9:78:40:78:fa:1a:7c:b8:49:cc:  
d2:3a:5c:5b:07:06:1e:1a:38:e2:6f:3a:95:d9:33:18:f3:8f:  
71:4a:0f:19:3e:06:f9:cb:bd:d1:0a:90:2e:2a:58:a5:a8:fa:  
16:50:5e:d0

**Kuva 8. Väestörekisterikeskuksen Jyrki Kataiselle myöntämä X.509v3-standardia noudattava varmenne. Keskeisimpiä varmenteen tietueita on lihavoitu ja täydennetty kurssiiveilla huomautuksilla.**

Julkisen avaimen järjestelmällä tarkoitetaan niitä toimenpiteitä ja käytäntöjä, joiden perusteella julkisen avaimen tietoverkossa kohtaava voi varmistaa vastaavan yksityisen avaimen haltijan yksilöivän tunnisteiden. Julkisen avaimen järjestelmän keskeisin toimija on varmentaja, joka kantaa vastuun varmenteiden myöntämisestä ja julkisen avaimen järjestelmän toiminnasta kokonaisuutena. Varmentajan keskeinen apulainen on rekisteröijä (registration authority), joka vastaa varmennetta hakevan henkilön ensitunnistuksesta esimerkiksi kasvotusten. Varmentajan myönnettyä varmenteen se julkaistaan yleensä julkisessa varmennehakemistossa, josta Pekka ja muut varmennetta tarvitsevat sen saavat.

Varmenteen haltijan – Liisan – tehtävä on säilyttää yksityistä avaintaan huolellisesti. Jos avain kuitenkin hukkuu tai joku siihen sisältyvä tieto vanhenee kesken varmenteen voimassaoloajan, varmenteen haltijalla on velvollisuus asettaa varmenne sulkulistalle (certificate revocation list). Varmenteeseen luottava taho – Pekka, tai Liisan autentikointia haluava palvelin – tarkistaa varmenteen voimassaolon sulkulistalta ennen varmenteen hyväksymistä. Kaikkien osapuolten toiminta ja vastuut on dokumentoitu varmennepolitiikassa, jonka varmentaja julkaisee.

Kuten todettu, julkisen avaimen salausmenetelmän edellyttämät laskutoimitukset ovat niin monimutkaisia, että Liisa ei suoriudu niistä päässään eikä ruutupaperilla. Siksi yksityinen avain käytännössä talletetaan tiedostoksi tietokoneen levyille, ja tarvittavat laskutoimitukset suoritetaan tietokoneen prosessorilla. Liisa voi esimerkiksi tallentaa yksityisen avaimensa ja siihen liittyvän varmenteen selaimessaan tai käyttöjärjestelmässään olevaan säilöön, jossa se on tarvittaessa mainittujen ohjelmistojen käytettävissä. Tällaista varmennetta kutsutaan ohjelmistovarmenteeksi (software certificate).

Ohjelmistovarmenteissa on kuitenkin joitain huonoja puolia. Levyjärjestelmään talletettu yksityinen avain voi paljastua haittaohjelman tai käyttäjän erehdyksen vuoksi. Käyttäjä itse ei kuitenkaan välttämättä huomaa tai tiedä, että hänen yksityinen avaimensa on paljastunut ja hänen tulee asettaa varmenne sulkulistalle. Parempi suojaus yksityiselle avaimelle saadaan, kun se siirretään turvamoduliin (hardware security module, HSM), joka on tietokoneesta erillinen, tietoja laitteistotasolla suojaava väline. Jos turvamoduli sisältää tallennuskapasiteetin lisäksi laskentakapasiteettia, ei yksityisen avaimen tarvitse poistua turvamodulista edes avaimella tehtäviä laskutoimituksia varten<sup>4</sup>.

Yksi turvamoduli, johon yksityinen avain voidaan tallettaa, on toimikortti (älykortti, sirukortti, suoritinkortti, engl. smart card). Toimikortti on luottokortin kokoinen tietokone, jonka rakenne on suunniteltu suojaamaan sen sisältämää tietoa ja elektroniikkaa ulkoisilta tunkeutumisyrityksiltä. Toimikortti on suhteellisen edullinen laite, joka pienen kokonsa

<sup>4</sup> On kuitenkin hyvä huomata, että vaikka yksityinen avain onkin suojassa, turvamodulille tulevat komennot, kuten käskyn allekirjoittaa tietty viesti, lähettää tietokone, joka yleensä ei ole yhtä hyvin suojattu kuin turvamoduli.

vuoksi kulkee mukavasti haltijansa lompakossa. Kun yksityistä avainta halutaan käyttää, kortti työnnetään tietokoneeseen kytkettyyn kortinlukijaan, joka asioi kortin kanssa sen pinnassa olevien kontaktipintojen kautta tai kontaktittomasti. Yleensä kortti aktivoidaan antamalla PIN-koodi tietokoneen tai kortinlukijan näppäimistöltä. Markkinoilla on myös toimiavaimia, joissa kortin ja kortinlukijan toiminnallisuus on integroitu yhdeksi, suoraan USB-väylään työnnettäväksi kokonaisuudeksi.

Suomessa kenties tunnetuin toimikorttiin nojaava julkisen avaimen järjestelmä on poliisin myöntämä kansalaisille tarkoitettu henkilökortti, johon upotetulle sirulle Väestörekisterikeskus myöntää varmenteen (Kuva 9). Sähköisessä henkilökortissa varmentajana on Väestörekisterikeskus, ja rekisteröijän tehtäviä hoitaa poliisi. Kansalaisen yksilöivänä tunnisteena varmenteessa käytetään hänen sähköistä asiointitunnustaan (katso luku 3.3). Toimikorttiin nojaavia julkisen avaimen järjestelmiä on toteutettu myös organisaatioiden sisäiseen käyttöön (esimerkiksi Kuva 8, jossa organisaationa on Valtioneuvoston kanslia), jolloin varmenteen haltijat ovat organisaation työntekijöitä.



**Kuva 9.** Poliisin myöntämän henkilökortin siru sisältää haltijansa yksityisen avaimen sekä Väestörekisterikeskuksen myöntämän kansalaisvarmenteen. Kuva: Poliisi.

Julkisen avaimen järjestelmien yleistymistä on jarruttanut käytettävyys. Peruskäyttäjät kokevat julkisen ja yksityisen avaimen käsitteet hankaliksi ymmärtää. Vaikka yksityisen avaimen sijoittaminen toimikortille tekee siitä hieman kouriintuntuvamman, eivät nekään ole saaneet laajaa suosiota varsinkaan yritysratkaisujen ulkopuolella. Loppukäyttäjät ovat kokeneet kortinlukijoiden ja lukijaohjelmistojen hankkimisen ja asentamisen työasemiinsa hankalaksi. Koska esimerkiksi julkishallinnon sähköisiin asiointipalveluihin voi kirjautua myös verkkopankkien tutuilla kertakäyttösalausanoilla, ovat sähköisen henkilökortin käyttömäärät Suomessa jääneet vähäisiksi.

Lisätietoa: Linden: Julkisen avaimen järjestelmä, toimikortit ja niiden soveltaminen organisaatiossa. Lisensiaatintutkimus, 2003.

Matkapuhelinverkoissa toimikorttia on käytetty liittymänhaltijan tunnistamiseen GSM-tekniikasta alkaen. Vaikka puhelimen sisälle työnnettävä liittymäkortti (subscriber identity module, SIM) perustuukin julkisen avaimen salauksen sijaan symmetriseen salaustenmenetelmään, ovat operaattorit tuoneet samalle kortille SIM-sovelluksen rinnalle yksityisen avaimen, johon liittyvän varmenteen antaa teleoperaattori. Mobiilivarmenteesta on tehty matkapuhelinasiakkaiden lisäpalvelu, jota myydään sekä suljettuun ympäristöön yritysratkaisuna että kuluttajien tunnistamiseen.

Mobiilivarmenne perustuu ETSI 102 204 ja 102 207 –standardeihin ja näiden suomalaisen soveltamisohjeeseen. Erillistä kortinlukijaa ja kortinlukijaohjelmistoa ei

tarvita. Käyttäjä antaa tunnistusta pyytävälle palvelimelle puhelinnumeronsa tai esimerkiksi käyttäjätunnuksensa, johon liittyvä puhelinnumero on organisaation identiteettihallinnan tiedossa. Tunnistusta pyytävä palvelu lähettää operaattorin tarjoamaan rajapintaan tunnistuspyynnön, jonka operaattori välittää tekstiviestikanavaa pitkin matkapuhelimen liittymäkortille. Liittymäkortti pyytää puhelimen käyttöliittymän kautta käyttäjää syöttämään yksityisen avaimen aktivoivan PIN-koodin, ja oikean koodin saatuaan liittymäkortti allekirjoittaa vastauksen tunnistuspyyntöön, jonka teleoperaattori välittää tunnistusta pyytäneeseen palveluun. Mobiilivarmennearkkitehtuuriin sisältyy myös roaming –toiminnallisuus, joka mahdollistaa eri teleoperaattorien mobiilivarmenteiden ristiinkäytön.

Lisätietoa: Ficom ry:  
Soveltamisohje ETSI:n MSS-standardeille

#### 4.6. Biometrinen tunnistus

Biometrinen tunnistus perustuu johonkin henkilön yksilölliseen anatomiseen tai fysiologiseen ominaisuuteen, joka säilyy muuttumattomana, vaikka henkilön ulkonäkö muuten voikin muuttua esimerkiksi ikääntymisen, lihomisen tai meikkauksen vuoksi. Sormenjalkia on käytetty rikostutkinnassa 1800-luvulta asti ja erilaisia asiakirjoja on allekirjoitettu kirjoitustaidon yleistymisestä alkaen. Passeissa, henkilöllisyystodistuksissa ja ajokorteissa valokuvaa käytetään laajasti haltijansa tunnistamiseen.

Tietotekniikassa biometrinen tunnistus voi perustua sormenjalkien, kasvojen tunnistuksen ja allekirjoituksen lisäksi esimerkiksi kädenmuotoihin, silmän väriä eli iriksen skannaukseen, äänentunnistukseen tai tapaan, jolla henkilö naputtelee tietokoneen näppäimistöä. Kun tunnistettava henkilö hakee tunnistusvälinettä (enrollment), hänestä talletetaan tunnistavan järjestelmän muistiin mallinne, johon tunnistushetkellä otettava näyte verrataan. Jos käytetty tunnistusalgoritmi tulee siihen johtopäätökseen, että näyte ja mallinne kuuluvat samalle henkilölle, on henkilön identiteetti todennettu onnistuneesti.

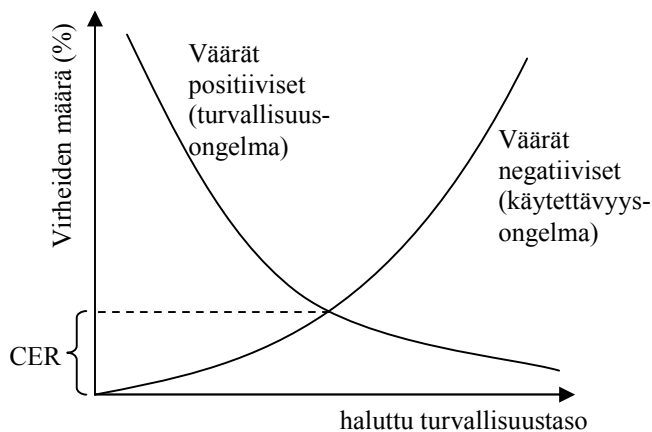
Salasanatunnistuksessa käyttäjän syöttämä salasana on joko oikein, tai muussa tapauksessa se on väärin. Biometrisen tunnistuksen luonteenpiirre on kuitenkin aina jonkinasteinen epävarmuus tunnistuksen tuloksen suhteen, mikä seuraa niistä olosuhteista, joissa mallinne ja näyte on otettu. Esimerkiksi sormenjalkitunnistuksessa algoritmin pitää huomioida, että sormi voi olla tunnistushetkellä hieman likainen tai eri asennossa, jolloin mallinne ja näyte eivät täysin vastaa toisiaan. Sen vuoksi biometrisessä tunnistuksessa joudutaan tyytymään siihen, että tunnistusalgoritmin mielestä näyte ja mallinne kuuluvat esimerkiksi 99 % todennäköisyydellä samalle henkilölle.

<b>OK.</b> Todellisuudessa mallinne ja näyte kuuluvat samalle henkilölle. Tunnistusalgoritmin mielestä tunnistus on onnistunut.	<b>Väärä positiivinen.</b> Todellisuudessa mallinne ja näyte kuuluvat eri henkilölle, mutta tunnistusalgoritmin mielestä tunnistus on onnistunut.
<b>Väärä negatiivinen.</b> Todellisuudessa mallinne ja näyte kuuluvat samalle henkilölle, mutta tunnistusalgoritmin mielestä tunnistus epäonnistui.	<b>OK.</b> Todellisuudessa mallinne ja näyte kuuluvat eri henkilölle. Tunnistusalgoritmin mielestä tunnistus epäonnistui.

Kuva 10. Väärät positiiviset ja väärät negatiiviset ovat biometrisen tunnistuksen keskeinen piirre.

Oheinen nelikenttä (Kuva 10) kuvaa syntyvää tilannetta ja niitä kahta tapaa, jolla biometrinen tunnistus voi mennä pieleen. Tunnistusalgoritmin mielestä tunnistus saattaa olla onnistunut, vaikka tosiasialla mallinne ja näyte kuuluvat eri henkilöille (ns. väärä positiivinen, false positive). Vastakohta on, että tunnistusalgoritmin mielestä tunnistus ei onnistunut, vaikka mallinne ja näyte tosiasialla ovat samalta henkilöltä (ns. väärä negatiivinen, false negative).

Väärin positiivisten ja negatiivisten ilmenemisen välillä vallitsee yhteys (Kuva 11); jos väärin positiivisten ilmenemistä halutaan vähentää, kasvaa samalla myös väärin negatiivisten määrä. Biometrisen tunnistuksen rakentaja joutuu siis tasapainoilemaan tunnistuksen luotettavuuden (väärät henkilöt hylätään mahdollisimman usein) ja käytettävyyden (oikeita henkilöitä hylätään mahdollisimman harvoin) välillä.



**Kuva 11. Väärin positiivisten ja negatiivisten yhteys. Mitä pienempi Cross-over error rate (CER), sitä paremmasta biometrisestä tunnistusmenetelmästä on kysymys.**

Biometristen tunnistusmenetelmien paremmuutta voidaan vertailla sen perusteella, missä pisteessä väärin positiivisten ja negatiivisten käyrät leikkaavat (Cross-over error rate, CER). Mitä pienempi CER-arvo on (eli mitä alempana leikkauspiste on oheisessa kuvassa) sitä luotettavammasta biometrisestä tunnistustavasta on kyse. Esimerkiksi biometrinen tunnistustapa, jonka CER=3% on parempi kuin tunnistustapa, jonka CER=4%.

Toinen periaatteellinen kysymys on, käytetäänkö biometristä tunnistusta käyttäjän tunnistena (erottamaan henkilö vertaisistaan eli vastaamaan kysymykseen ”kuka tämä henkilö on”) vai käyttäjän identiteetin todentamiseen (autentikointiin, eli vastaamaan kysymykseen ”Onko tämä henkilö käyttäjä X”). Jälkimmäisessä tapauksessa biometrinen tunnistus pelkästään syrjäyttää salasanan tai toimikortin PIN-koodin, ensimmäisessä vaihtoehdossa myös käyttäjän yksilöivän tunnisteen. Kun käyttäjäpopulaatio kasvaa, biometrisen tunnistuksen käyttö käyttäjän tunnistena käy epävarmaksi. Tämä johtuu siitä, että suuressa populaatiossa on todennäköistä, että otetun näytteen voidaan käytetyn tunnistusalgoritmin epävarmuuden puitteissa tulkita täsmäävän useampaan kuin yhteen mallinteeseen.<sup>5</sup>

<sup>5</sup> Tämä on ruumiillistuma niin sanotusta syntymäpäiväparadoksista, joka on tilastotieteilijöille tuttu ongelma: kuinka monta opiskelijaa luokassa pitää olla, että yli 50% todennäköisyydellä löytyy ainakin kaksi henkilöä, jotka viettävät syntymäpäiväänsä samana päivän. Vastaus on 23 opiskelijaa, mitä monet pitävät maalaisjärjellä ajateltuna yllättävän pienenä lukuna.

Suomessakin huomiota saanut biometrisen tunnistuksen käytännön sovellus on biometrinen passi. Vuodesta 2009 lähtien passit ovat sisältäneet haltijansa muiden henkilötietojen lisäksi kasvokuvan ja sormenjäljet, jotka voidaan lukea langattomasti passista RFID-tekniikan avulla. Luettavien tietojen eheys on varmistettu digitaalisella allekirjoituksella ja luottamuksellisuus symmetrisellä salausavaimella, joka on johdettavissa passin henkilötietosivulle tulostetusta koneluettavasta kentästä. Näin passitarkastuksessa rajavartija voidaan syrjäyttää automaattilla, joka lukee haltijansa kasvokuvan passista ja vertaa sitä automaatin kameran ottamaan kuvaan.

Yhteiskunnallisessa keskustelussa biometriseen tunnistukseen on yhdistetty huoli yksityisyyden suojasta. Toisin kuin vaikkapa salasanatunnistus, biometrinen tunnistus voidaan tehdä myös henkilön tietämättä ja ilman hänen suostumustaan esimerkiksi julkisella paikalla olevalla valvontakameralla. Biometrisen tunnistuksen sosiaalinen hyväksyttävyyys voi myös tulla ongelmaksi; Euroopassa sormenjäljet on perinteisesti liitetty rikostutkintaan. Loppukäyttäjä voi myös kokea vastenmielisyyttä biometrisen tunnistuksen tekeviä skannereita kohtaan, jos kokee operaation epämiellyttäväksi tai tunkeilevaksi.

Jos salasana tai varmenne joutuvat yksittäistapauksissa väärinkäytön kohteeksi, ne voidaan vaihtaa tai asettaa sulkulistalle. Myös väärinkäytetty luottokorttinumero tai jopa henkilötunnus voidaan vaihtaa, mutta henkilö ei voi vaihtaa biometristä ominaisuuttaan. Niinpä biometrisen tunnistusmenetelmän käyttökelpoisuus uhkaa murentua, jos identiteettivargaat keksivät menetelmän<sup>6</sup>, jolla biometristä tunnisteita pystytään kopioimaan ilman, että kopion käyttäminen huomataan tunnistushetkellä. Tämä näkökulma on tarpeen huomioida erityisesti silloin, kun tunnistusta ei tehdä tunnistajan valvonnassa vaan esimerkiksi verkon yli.

#### **4.7. Kertakirjautuminen**

Kertakirjautuminen (single sign-on, SSO) on käsite, joka tulee usein esille identiteetin- ja pääsynhallinnan projekteissa. Ketäpä ei harmittaisi, kun työnteke keskeytyy tietokoneen pyytäessä syöttämään käyttäjätunnusta ja salasanaa.

Kertakirjautuminen tarkoittaa, että käyttäjän tarvitsee tunnistautua (esimerkiksi syöttää käyttäjätunnus ja salasana) vain kerran, ja sen jälkeen kaikki kertakirjautumisen piirissä olevat palvelut avautuvat käyttäjälle ilman uutta tunnistautumista. Kertakirjautuminen ei siis ole oma tunnistusmenetelmänsä eikä myöskään tunnistusta syrjäyttävä järjestely, vaan ikään kuin askel eteenpäin autentikoinnista; salasana tarvitsee syöttää vain kerran, jonka jälkeen se on ”voimassa” istunnon loppuun<sup>7</sup> asti. Kertakirjautuminen on eri asia kuin yhden käyttäjätunnuksen ja salasanan periaate, jossa palvelut ovat kyllä yhden ja saman käyttäjätunnuksen ja salasanan takana, mutta ne tulee syöttää kuhunkin palveluun aina erikseen.

---

<sup>6</sup> Esim. Mythbusters, Fingerprints busted: <http://www.youtube.com/watch?v=MAfAVGES-Yc>

<sup>7</sup> Kertakirjautumisen käänteisoperaatio on kertauloskirjautuminen (single logout), jossa käyttäjän istunnot kaikissa palveluissa päätetään yhtä aikaa. Hajautetussa ympäristössä, jossa käyttäjällä on toisistaan riippumattomia istuntoja eri palveluihin, täydellinen kertauloskirjautuminen on usein haastavampi toimenpide kuin kertasisäänkirjautuminen.



Paikallinen (esim. ESSO)	näennäiskertakirjautuminen	Palvelinpohjainen kirjautuminen (esim. web proxy)	näennäiskerta-
Paikallinen (esim. PKI)	aito kertakirjautuminen	Palvelinpohjainen aito kertakirjautuminen (esim Kerberos)	

**Kuva 12. Nelikenttä kertakirjautumisen toteutusperiaatteista.**

Kertakirjautuminen voidaan toteuttaa eri periaatteilla, joita on kuvattu oheisessa nelikentässä. **Näennäiskertakirjautumisessa** (pseudo single sign-on) käyttäjän ja tunnistusta vaativan palvelun välissä on väliohjelmisto, joka välivarastoi käyttäjän käyttäjätunnuksia ja salasanoja, ja kirjautumishetkellä antaa ne tunnistusta vaativalle palvelulle loppukäyttäjää asialla häiritsemättä. Loppukäyttäjän tarvitsee vain istunnon alussa kirjautua väliohjelmistoon, joka voi sijaita joko käyttäjän päätelaitteessa (paikallinen näennäiskertakirjautuminen) tai kertakirjautumisesta huolehtivalla palvelimella, jonka läpi yhteydet ohjataan (palvelinpohjainen kertakirjautuminen). Näennäiskertakirjautumisen etuna on nopea käyttöönotto, koska varsinaisia tunnistusta vaativia palveluita ei tarvitse muuttaa. Palvelut eivät tiedä eikä niiden edes tarvitse tietää, että käyttäjätunnus ja salasana tulivat itse asiassa väliohjelmistosta eikä loppukäyttäjältä. Edistyneet väliohjelmistot osaavat myös omatoimisesti vaihtaa käyttäjän salasanan, jos palvelu edellyttää salasanan säännöllistä vaihtamista.

Myös **aidossa kertakirjautumisessa** (true single sign-on) on väliohjelmisto, joka tunnistaa käyttäjän istunnon alussa. Väliohjelmistossa ei kuitenkaan ole käyttäjätunnusten ja salasanojen välivarastoa, vaan sen sijaan tunnistusta vaativan palvelun ohjelmakoodia muutetaan niin, että palvelu luottaa väliohjelmiston tekemiin tunnistussanomoihin (ticket, assertion), jotka välittävät palvelulle tunnistetun käyttäjän identiteetin. Väliohjelmisto voi sijaita käyttäjän päätelaitteessa (paikallinen aito kertakirjautuminen) tai erityisellä tunnistuspalvelimella (palvelinpohjainen aito kertakirjautuminen).

Klassinen esimerkki palvelinpohjaisesta aidosta kertakirjautumisesta on Kerberos, joka perustuu Needham-Schröderin tunnistusprotokollaan. Käyttäjän tunnistamisen suorittaa erityinen avaintenjakopalvelin (Key Distribution Center, KDC), joka välittää symmetrisen istuntoavaimen käyttäjälle ja tunnistusta vaativalle palvelimelle. Koska kyse on aidosta kertakirjautumisesta, tunnistukseen nojaava palveluun tarvitsee asentaa Kerberos-tunnistuksen mahdollistava moduuli eli palvelu tarvitsee kerberoida. Laajimmin käytetty Kerberos-toteutus on Windowsissa, jonka toimialuekirjautuminen perustuu Kerberos-protokollaan.

Edellä luvussa 4.5 käsiteltiin julkisen avaimen järjestelmää, joka mahdollistaa käyttäjän tunnistamisen hänen päätelaitteessaan olevan yksityisen avaimen avulla. Yksityiseen avaimeen perustuva tunnistus on esimerkki aidosta paikallisesta kertakirjautumisesta. Tunnistus tapahtuu käyttäjän päätelaitteeseen asennetun yksityisen avaimen ja sen käyttöön tarvittavan ohjelmiston (ja mahdollisen laitteiston kuten toimikortin) avulla. Myös tunnistusta vaativa palvelun on tuettava jotain julkisen avaimen menetelmään perustuvaa tunnistusprotokollaa.

WWW-ympäristön kertakirjautumiseen on olemassa palvelinpohjaisia tuotteita, jotka perustuvat WWW-edustapalvelimeen eli -proxyyn. WWW-proxyssä kaikki selaimesta ulos lähtevä liikenne ohjataan proxyyn, josta se välitetään edelleen Internetiin. WWW-proxyllä voidaan toteuttaa palvelinpohjainen näennäiskertakirjautuminen: WWW-proxy

tunnistaa käyttäjän, hakee tietokannastaan käyttäjän käyttäjätunnuksen ja salasanan, ja antaa ne käyttäjän puolesta tunnistusta vaativaan palveluun.

Markkinoilla on saatavilla runsaasti organisaatiokertakirjautumiseen tarkoitettuja tuotteita (Enterprise Single Sign-on, ESSO), jotka perustuvat käyttäjän työasemaan asennettavaan ohjelmistokomponenttiin. ESSO:n avulla voidaan toteuttaa kertakirjautuminen myös muihin kuin WWW-palveluihin. Käyttäjä tunnistetaan kun hän kirjautuu työasemalle. Sen jälkeen ESSO-väliohjelmisto tarkkailee työaseman käyttöliittymää, ja sisäänkirjautumisruudun havaitessaan käy kirjoittamassa siihen oikean käyttäjätunnuksen ja salasanan automaattisesti. ESSO on esimerkki paikallisesta näennäiskertakirjautumisesta.

#### **4.8. Lopuksi**

Lopuksi todettakoon, että identiteetin- ja pääsynhallinnan kirjossa käyttäjän sähköinen tunnistus on ehkä luonteeltaan teknisin kokonaisuus, joka voidaan toteuttaa ”kaupan hyllyiltä” saatavilla erilaisilla teknisillä välineillä. Toisaalta juuri autentikointi – käyttäjätunnusta ja salasanaa pyytävä tietokone – on varsin konkreettinen ja helposti ymmärrettävä asia myös identiteetin- ja pääsynhallintaan vihkiytymättömille henkilöille. On suuri houkutus ajatella, että identiteetin- ja pääsynhallintaa voidaan kohentaa syrjäyttämällä salasanatunnistus vahvalla tunnistuksella. Vaikka vahva tunnistus onkin tarpeen tietyissä käyttötilanteissa, löytyvät identiteetin- ja pääsynhallinnan keskeisimmät kehityskohteet usein kuitenkin muualta. Niin kuin tietoturvallisuudessa yleensä, myös käyttäjän tunnistuksen menetelmää valittaessa kannattaa tasapainottaa vahvan tunnistuksen käyttöönotosta ja ylläpidosta koituvia kustannuksia niiden kustannusten kanssa, jotka syntyvät realisoituvista riskeistä silloin, kun heikko tunnistus pettää.

#### **4.9. Pohdittavaa**

- Käyttäjän tunnistus tapahtuu salasanalla ja tekstiviestinä hänen matkapuhelimeensa toimitettavalla kertakäyttösalasanalla. Täytyykö lain määritelmä vahvasta sähköisestä tunnistamisesta?
- Millainen voisi olla palvelu, jossa heikko ensitunnistus riittää mutta jossa tarvitaan vahvaa autentikointia?
- Julkisen avaimen järjestelmän ja toimikorttien kohdalla huomautettiin, että vaikka toimikortti tarjoaakin melko hyvän suojan sisältämälleen tiedolle, toimikortti ottaa vastaan komentoja tietokoneelta, johon toimikortti on kytketty. Minkälaisia riskejä tähän sisältyy? Minkälaista vahinkoa tietokoneeseen pesiytynyt haittaohjelma voi saada aikaan?

## 5. Käyttövaltuuksien hallinta eli auktorisointi

Kun käyttäjä on tunnistettu, tulee seuraavaksi ratkaistavaksi kysymys, onko käyttäjällä valtuus eli oikeus suorittaa hänen pyytämänsä toiminto. Tällöin kysymys on pääsynvalvontapäätöksestä (access control decision), johon huipentuu käyttövaltuuksien (käyttöoikeuksien) hallinnaksi eli auktorisoinniksi (authorisation) kutsuttu prosessi. Yhdessä käyttäjän tunnistuksen kanssa pääsynvalvontapäätös muodostaa pääsynvalvonnan (access control) kutsutun toimintasarjan, joka tapahtuu sillä hetkellä kun käyttäjä kirjautuu palveluun. Pääsynvalvonta on edelleen keskeinen osa pääsynhallintaa (access management), joka sisältää lisäksi käyttäjien käyttövaltuuksien hallinnan.

Tässä luvussa esitellään ensin pääsynvalvonnan määritelmä ja sitten tavallisimpia pääsynvalvontamalleja. Lopuksi esitellään keskeisimpiä käyttövaltuuksien (eli käyttöoikeuksien) hallinnan periaatteita.

### 5.1. Määritelmä

Formaalisti pääsynvalvonnassa on kyse funktiosta

$f(S,O,A,e)$

jossa

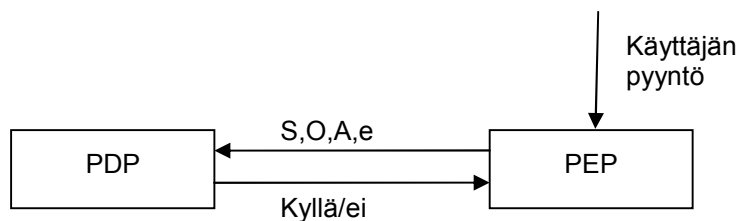
S (subject) on tunnistettu loppukäyttäjä,

O (object) on suojattava kohde (esim. tiedosto), johon käyttäjä haluaa suorittaa toiminnon,

A (action) on toiminto (esim. lue), jonka käyttäjä haluaa suorittaa ja

e (environment) on kokoelma ympäristöä koskevia tekijöitä, joilla on vaikutusta pääsynvalvontapäätökseen (esimerkiksi verkko, josta käyttäjä tulee ja kellonaika)

Parametriensa arvoista riippuen funktio  $f$  tuottaa joko arvon kyllä tai ei, eli pääsy joko sallitaan tai evätään.



**Kuva 13. Pääsynvalvontapäätöksen tekeminen (PDP) ja täytäntöönpano (PEP).**

Usein pääsynvalvontapäätöksen tekeminen ja sen edellyttämät päättelyt on leivottu sisään siihen palveluun, johon käyttäjä kirjautuu. Pääsynvalvontapäätöksen tekeminen voidaan myös irrottaa omaksi, keskitetyksi palvelukseen (Kuva 13). Tällöin pääsynvalvontapäätöksen tekevää komponenttia kutsutaan PDP:ksi (Policy decision point), ja tehdyn päätöksen täytäntöönpanevaa komponenttia PEP:ksi (Policy enforcement point). PEP välittää pääsynvalvontapäätökseen vaikuttavat tiedot PDP:lle, joka palauttaa PEP:lle pääsynvalvontapäätöksen, jonka PEP toteuttaa. Suojattavan kohteen pääsynvalvontasäännöt voidaan esimerkiksi kuvata XACML-kielen avulla (Extensible Access Control Markup Language).

Pääsynvalvonnassa lähtökohtana on, että käyttäjä on tavalla tai toisella tunnistettu – se, millä tavalla, ei ole pääsynvalvonnassa enää mielenkiintoista. Usein käyttäjätunnistus on suoritettu ”riittävän luotettavasti”, mutta jos käyttäjille on käytettävissä erivahvuisia tunnistusmenetelmiä, voidaan ajatella, että jotkut käyttäjät, suojattavat kohteet tai toiminnot edellyttävät muita vahvempaa tunnistusta. Tällöin tunnistuksen vahvuus on yksi pääsynvalvontapäätökseen vaikuttava käyttäjän attribuutti, joka voidaan ilmaista vaikka jollain luvussa 4.3 esiteltyllä viitekehyksellä.

## 5.2. Pääsynvalvontamatriisi

Pääsynvalvontamatriisi (Access control matrix) on klassinen tapa esittää käyttäjän käyttövaltuudet suojattavaan kohteeseen. Suojattavat kohteet esitetään matriisin sarakkeissa, ja käyttäjät riveillä. Matriisin soluihin kirjataan toiminnot, jotka kullekin käyttäjälle on sallittu kyseiseen suojattavaan kohteeseen.

	/home/pekka/foo	/tmp/bar	/etc/passwd
Pekka	read, write	read	-
Liisa	read	read,write	-

**Taulukko 1. Esimerkki pääsynvalvontamatriisista.**

Oheisessa taulukossa on esimerkki pääsynvalvontamatriisista, joka tässä tapauksessa on perinteinen Unix-tiedostojärjestelmä. Pekka-nimisellä käyttäjällä on kotihakemistonsa tiedostoihin luku- ja kirjoitusoikeus. Liisa-nimisellä käyttäjällä on tiedostoon pelkästään lukuoikeus. Sen enempää Pekka kuin Liisa eivät kuitenkaan voi lukea tai kirjoittaa tiedostoa /etc/passwd.

Pääsynvalvontamatriisin yhtä saraketta kutsutaan pääsynvalvontalistaksi (Access control list, ACL), ja se kertoo, mitä eri käyttöoikeuksia eri käyttäjillä on tähän suojattavaan kohteeseen. Vastaavasti pääsynvalvontamatriisin yhtä riviä kutsutaan käyttäjän valmiuksiksi (capabilities), jotka kertovat, mitä eri käyttöoikeuksia tällä käyttäjällä on.

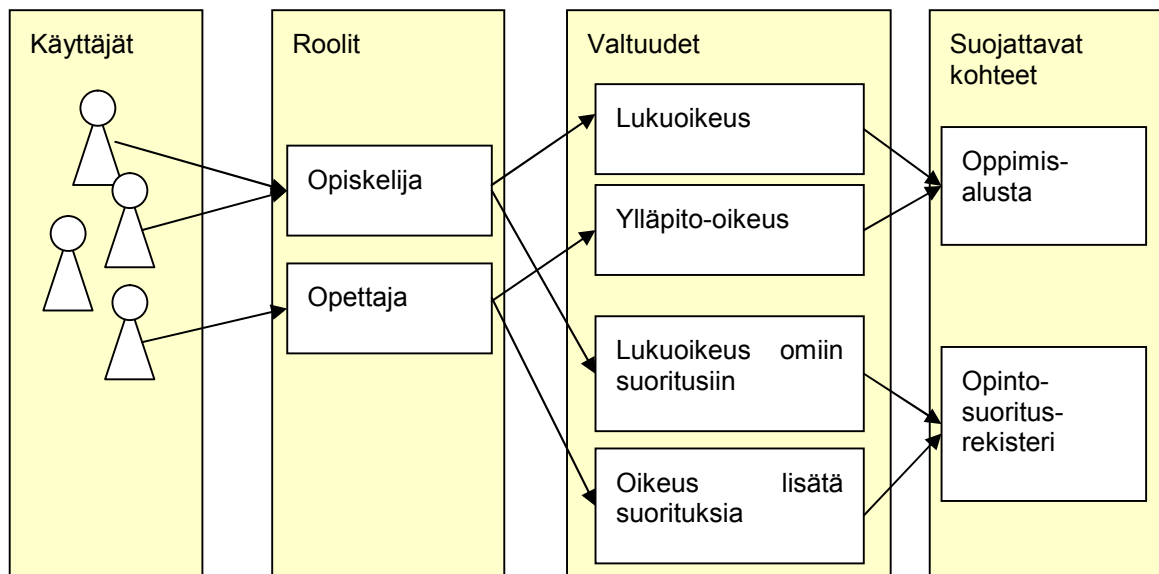
Pääsynvalvontamatriisin haittapuoli on, että sen koko kasvaa pian hallitsemattomaksi, kun käyttäjien ja suojattavien kohteiden määrä kasvaa. Organisaation käyttäjät, suojattavat kohteet, käyttövaltuuden perusteena oleva toiminnot ja projektit vaihtuvat usein, mikä tekee pääsynvalvontamatriisin ylläpitämisestä ylivoimaisen tehtävän. Siksi onkin kehitetty muita pääsynhallintamalleja, jotka pyrkivät vähentämään pääsynvalvontamatriisin kompleksisuutta. Niistä seuraavana tutustutaan nykyisin laajasti käytettyyn rooliin perustuvaan pääsynvalvontaan.

## 5.3. Rooliin perustuva pääsynvalvonta

Rooliin perustuvassa pääsynvalvonnassa (role-based access control, RBAC) käyttäjän ja käyttövaltuuden väliin on luotu roolin abstraktio: käyttäjälle annetaan rooleja, jotka kuvaavat esimerkiksi hänen työtehtäviään organisaatiossa. Käyttövaltuudet puolestaan annetaan rooleille. Yksittäisen käyttäjän käyttövaltuus saadaan selvitettyä, kun ensin selvitetään käyttäjällä olevat roolit, ja sen jälkeen tarkastellaan, millaisia valtuuksia kyseisiin rooleihin on liitetty.

Oletetaan, että korkeakoulussa on kurssi nimeltä ”Identiteetin- ja pääsynhallinta”. Korkeakoulun roolimalli sisältää seuraavat kurssia koskevat roolit: opettaja ja opiskelija. Opettajan tehtävänä on valmistella ja pitää luennot sekä laatia tentit ja arvostella

opintosuoritukset. Opiskelijoiden tehtävä on opiskella ja käydä kurssin tentissä. Lisäksi kurssiin liittyy kaksi suojattavaa kohdetta: oppimisalusta ja opintosuoritusrekisteri.



**Kuva 14. Esimerkki rooliin perustuvasta pääsynvalvonnasta.**

Opiskelijaroolin haltijalla on valtuudet käyttää oppimisalustaa lukuoikeuksin<sup>8</sup>, mutta vain kurssin opettajaroolin haltijalla on valtuus ylläpitää ja päivittää kurssialuetta oppimisalustassa. Kun kurssi on päättynyt ja opettaja on arvostellut suoritukset, hänellä on oikeus lisätä kurssia koskevia suorituksia opintosuoritusrekisteriin. Yksityisyyden suojan vuoksi opettajalla ei kuitenkaan ole lukuoikeuksia opintosuoritusrekisteriin – ei tämän eikä muidenkaan kurssin suorituksiin. Opiskelija itse sen sijaan voi käydä opintosuoritusrekisteristä tarkistamassa, minkä arvosanan hän sai kurssista.

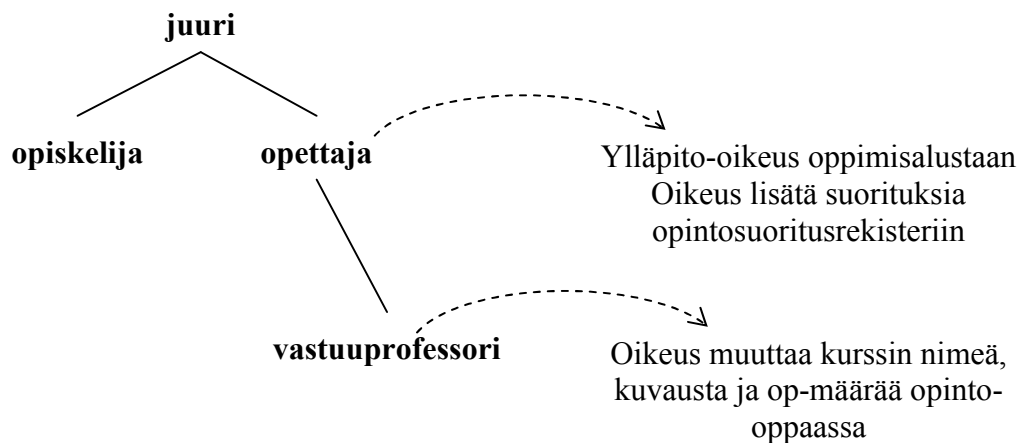
Tarkoituksenmukaisten roolien tunnistaminen organisaatiossa eli roolien louhinta (role mining) on rooliin perustuvan käyttövaltuushallinnan suunnittelun keskeinen vaihe. Roolimalli riippuu organisaation toiminnasta. Tyypillisiä rooleja ovat esimerkiksi kuuluminen tiettyyn organisaatioyksikköön, tietyn tehtävänimikkeen omistaminen, esimiesasema jne. Roolimallia rakennettaessa voidaan myös tehdä valintoja, jotka vaikuttavat suuresti syntyvien roolien määrään. Jos korkeakoulussa on esimerkiksi tuhat eri kurssia, onko korkeakoulussa myös tuhat eri opettajaroolia (”opettaja – identiteetin- ja pääsynhallinta”, ”opettaja – matematiikan peruskurssi 1”...) vai vain yksi rooli ”opettaja”, johon liitetään attribuuttina tieto siitä, mihin kurssiin opettajarooli liittyy?

Samalla henkilöllä voi olla yhtä aikaa useita rooleja; opiskelija voi suorittaa ja opettaja luennoida yhtä aikaa montaa eri kurssia. Rooleilla on myös alku ja loppu, joiden määrittelemineen liittyy roolien louhintaan; rooli kurssin opiskelijana alkaa tavallisesti siitä, kun opiskelija ilmoittautuu kurssille (ja ilmoittautuminen hyväksytään). Mutta koska opiskelijarooli kurssiin voidaan poistaa? Silloin kun opiskelija pääsee tentin läpi? Vai kun viimeinenkin tenttimahdollisuus on ohi? Vai tulisiko opiskelijalla olla kurssirooli aina hamaan valmistumiseensa asti, jotta hän tarvittaessa voi kerrata kurssin asioita? Vaikka roolien louhintaan on saatavilla työkaluja, roolien mallintaminen ja elinkaaren

<sup>8</sup> Käytännössä opiskelijalla on oppimisalustassa myös muitakin valtuuksia, kuten valtuus keskustella keskustelupalstalla tai palauttaa harjoitustöitä, mutta yksinkertaisuuden vuoksi ne on tässä sivuutettu.

määrittäminen sisältää usein rajankäyntejä, jotka edellyttävät organisaation toiminnan syvällistä ymmärtämistä.

Rooliin perustuvan pääsynhallinnan yksi piirre on roolien hierarkia ja periytyminen. Roolille voidaan määritellä lapsirooleja, jotka perivät kaikki vanhemmillaan olevat roolit ja siten rooleihin edelleen kytketyt käyttövaltuudet. Oletetaan, että jokaisella kurssilla on lisäksi vastuuprofessori, jolla on kaikki samat oikeudet kuin kurssin opettajalla. Lisäksi vastuuprofessorilla on oikeus muuttaa kurssin nimeä, kuvausta ja opintopistemäärää sähköisessä opinto-oppaassa. Tilannetta on havainnollistettu kuvan mukaisella roolipuulla.



**Kuva 15. Roolipuun rooleihin kytketyt valtuudet on esitetty katkoviivalla.**

Roolipuun juurirooli on kaikilla käyttäjillä, ja opiskelija ja opettaja ovat juuriroolin lapsirooleja. Jos juurirooliin on kytketty jokin käyttövaltuus, se on automaattisesti myös jokaisella opiskelijalla ja opettajalla (ja myös kaikilla niillä käyttäjillä, joilla ei opiskelija- ja opettajaroolia). Vastuuprofessori on opettajan lapsirooli. Henkilöllä, jolle on annettu vastuuprofessorirooli, on siis myös opettajarooli (ja juurirooli). Niinpä vastuuprofessorille kuuluu kaikki opettajalla olevat käyttövaltuudet (oppimisalustan ylläpito-oikeus ja suoritusten lisäysoikeus opintosuoritusrekisteriin). Lisäksi vastuuprofessori voi muuttaa kurssin nimeä, kuvausta ja opintopistemäärää opinto-oppaassa.

Roolihierarkia tuo joustavuutta rooliajatteluun. Jos huomataan, että organisaatiossa syntyy tarve myöntää lisävaltuuksia jonkun käyttäjäryhmän (=roolin) osajoukolle, voi lapsiroolin perustaminen kyseiselle osajoukolle poistaa tarpeen rinnakkaisen roolin (ja rooliin liittyvien käyttövaltuuksien) perustamiselle. Roolihierarkian rakentaminen edellyttää kuitenkin huolellista suunnittelua. Voitaisiinko esimerkiksi ajatella, että opettajarooli siirrettäisiin oppilasroolin lapsirooliksi?

#### 5.4. Muita pääsynvalvontamenetelmiä

Rooliin perustuvan pääsynhallinnan lähtökohtana on käyttäjille annetut roolit, joita ilman pääsynvalvontaa ei voida tehdä. Oletetaan, että palvelun käyttöoikeus on kaikilla täysi-ikäisillä henkilöillä, joiden kotipaikka on Tampere. Jotta rooliin perustuvaa pääsynvalvontaa voitaisiin käyttää, tulisi jokaiselle ehdon täyttävälle käyttäjälle ensin antaa rooli ”täysi-ikäinen tamperelainen”. Lisäksi rooli tarvitsee päivittää päivittäin, koska uusia täysi-ikäisiä tamperelaisia tulee joka päivä.

**Attribuuttiin perustuva pääsynvalvonta** (attribute-based access control, ABAC) laajentaa rooliin perustuvaa pääsynvalvontaa siten, että roolien sijaan pääsynvalvonta voi perustua mihin vain käyttäjän, palvelun, operaation tai ympäristön attribuuttiin. Pääsy voidaan esimerkiksi sallia, jos käyttäjän kotikunta on Tampere ja syntymäaika vähintään 18 vuotta sitten. Näin käyttäjälle ei tarvitse välttämättä luoda ylen määrin rooleja pääsynvalvontaa varten.

**Pakotettu pääsynvalvonta** (mandatory access control, MAC) lähtee siitä, että käyttöoikeuksien antaminen ei ole tiedoston tai resurssin omistajan vapaassa harkinnassa, vaan käyttöjärjestelmätasolla pakotettu toiminnallisuus. Lähtökohtana on, että tieto on turvaluokiteltu esimerkiksi tasoille erittäin salainen, salainen, luottamuksellinen ja rajoitettu. Käyttäjille on annettu vastaavat luokat. Käyttöjärjestelmä huolehtii, että esimerkiksi luottamuksellinen-tasolle turvaluokiteltu käyttäjä (tai hänen tunnuksellaan järjestelmään livahtanut haittaohjelma) voi lukea vain luottamuksellista ja rajoitettua tietoa. Kirjoittaa hän voi luottamuksellisia, salaisia ja erittäin salaisia asiakirjoja. Formaalisti nämä voidaan ilmaista kahdella säännöllä, jotka tunnetaan kehittäjiensä mukaan Bell-LaPadula-mallina:

- No read-up. Käyttäjä ei voi lukea tietoa, jonka turvaluokitus on hänen luokitustaan korkeampi.
- No write-down. Käyttäjä ei voi kirjoittaa tietoa, joka saa matalamman turvaluokituksen kuin käyttäjällä itsellään on.

Nämä kaksi sääntöä luovat järjestelmän, jossa korkeammat turvaluokat näyttäytyvät alemman turvaluokituksen käyttäjälle ”tiedon mustana aukkona”, joka imee sisäänsä kaiken käyttäjää korkeammalla turvaluokalla olevan tiedon, mutta josta ei koskaan tule mitään tietoa ulos.

Pakotettu pääsynvalvonta kehitettiin aikoinaan Yhdysvaltojen armeijan tarpeisiin, mutta muuten sen käytännön sovellukset ovat jääneet melko vähäisiksi. Aukottoman toteutuksen tekeminen on osoittautunut hankalaksi. Toisaalta pakotettu pääsynvalvonta on käytännössä kankea ja rajoittava toimintamalli, koska usein on kuitenkin tarpeen pystyä tuomaan tietoa hallitusti myös korkeammalta turvaluokalta matalampaan, mikä nakertaa koko pääsynvalvontamallin periaatetta. Teoreettisena mallina pakotettu pääsynvalvontamalli on kuitenkin merkittävä.

Viimeisenä pääsynvalvontamallina esitellään **jäljitettävyyteen perustuva pääsynvalvonta** (accountability based access control), joka ei oikeastaan ole pääsynvalvontamalli alkuunkaan. Jäljitettävyyteen perustuvan pääsynvalvonnan filosofiana on, että aukottoman pääsynvalvonnan toteuttaminen tunnustetaan ylivoimaiseksi. Pääsynhallinnasta tulisi niin monimutkainen ja kankea ja sen ylläpidosta niin työlästä, että siihen ei edes pyritä, vaan tyydytään rajaamaan käyttäjien käyttövaltuuksia hieman väljemmin. Pääsynhallintaa täydennetään tallentamalla käyttövaltuuksien käyttäminen lokiin, josta tulostettavia raportteja voidaan väärinkäytöksiä epäiltäessä tarkastella.

Jäljitettävyyteen perustuvan pääsynvalvontamallin ongelma on, että se ei noudata seuraavaksi esiteltävää vähimmän käyttövaltuuden periaatetta: se ei estä oikeudetonta käyttöä, eikä myöskään suojaa erehdyksiltä ja virheiltä. Siitä huolimatta pääsynvalvontamallia käytetään laajasti esimerkiksi viranomaisrekistereissä, kuten väestö- ja potilastietojärjestelmissä.

## **5.5. Vähimmän käyttövaltuuden periaate**

Vähimmän käyttövaltuuden periaate (least privilege) on eräs tietoturvallisuuden keskeisistä periaatteista. Sen mukaan käyttäjällä saa olla käytössään vain niin laajat käyttövaltuudet kuin mitkä hän tarvitsee hänelle kuuluvien tehtävien hoitamiseen. Koko käyttövaltuuksien mallintamisen ja hallinnan problematiikka rakentuukin tämän periaatteen ympärille; muutoinhan kaikille käyttäjille voitaisiin antaa aina kaikki valtuudet, ja sen kummempaa käyttövaltuuksien hallintaa ei tarvittaisi.

Vähimmän käyttövaltuuden periaate tarkoittaa myös sitä, että vaikka käyttäjälle olisi annettu laajat käyttövaltuudet, niitä käytetään vain silloin kun niitä tarvitaan. Vaikka käyttäjällä olisi käyttöjärjestelmään pääkäyttäjän (root) käyttövaltuudet, ne otetaan käyttöön vain silloin kun tehdään pääkäyttäjän käyttöoikeuksia edellyttäviä toimenpiteitä, ja muulloin tietokonetta käytetään peruskäyttäjän käyttöoikeuksilla. Näin vähimmän käyttövaltuuden periaate ehkäisee varsinaisten väärinkäytösten lisäksi myös inhimillisiä erehdyksiä ja virheitä.

Vähimmän käyttövaltuuden periaatetta rikotaan, jos organisaatio ei vaivaudu mallintamaan suojattavien kohteidensa käyttövaltuuksia riittävästi, vaan antaa käyttäjille ”varmuuden vuoksi” tarpeettoman suuret käyttövaltuudet (vrt. jäljitettävyyteen perustuva pääsynvalvonta, luku 5.4). Organisaatioiden toiminta ja käyttäjien käyttövaltuudet organisaatiossa ovat toki tosielämässä monimutkaisia, mutta edes keskeisimmät suojattavat kohteet olisi syytä tunnistaa ja suojata osana organisaation riskienhallintaa.

Eräs tyypillinen tilanne syntyy, kun työntekijä vaihtaa tehtäviään organisaation sisällä. Käyttäjän ja myös organisaation intressi on huolehtia, että käyttäjällä on uusien työtehtävien edellyttämät käyttövaltuudet. Sen sijaan käyttäjällä itsellään ei välttämättä ole painetta luopua aikaisempiin työtehtäviin liittyvistä käyttövaltuuksista, joten jos organisaatio ei huolehdi niiden poistamisesta, organisaation pitkäaikaisille työntekijöille kumuloituu vähitellen mittavat ylimääräiset käyttövaltuudet järjestelmiin. Jos käyttövaltuuksien raportointijärjestelmät ovat vajavaiset, ei organisaatiolla ja käyttövaltuuksien vastuuhenkilöillä välttämättä ole käsitystä käyttäjälle ”unohtuneista” valtuuksista. Valtuuksiin voi sisältyä esimerkiksi vaarallisia työyhdistelmiä, joihin tutustutaan seuraavaksi.

## **5.6. Vaarallisten työtehtävien eriyttäminen**

Taloushallinnossa on tiedetty jo vuosisatoja, että kassaa ja kirjanpitoa ei saa hoitaa yksi ja sama ihminen. Vaarallisten työtehtävien eriyttäminen (segregation of duties, SOD) kahdelle eri henkilölle ehkäisee työtehtävien hoidossa tapahtuvia erehdyksiä, virheitä ja väärinkäytöksiä. Sama pätee myös tietojärjestelmien käyttövaltuuksissa.

Sama henkilö ei saa sekä luoda että hyväksyä matkalaskua, koska henkilö voi altistua erehdyksiin, virheisiin tai väärinkäytöksiin omia matkalaskujaan hyväksyessään. Omien matkalaskujen hyväksyminen onkin tyypillisesti estetty matkalaskujen tekemiseen ja hallintaan tarkoitetuissa ohjelmistoissa.

Vaarallisia työtehtäviä saattaa kuitenkin löytyä myös taloushallinnon ulkopuolelta. Luvun 5.3 esimerkissä vaarallinen työyhdistelmä voi syntyä, jos kurssin opettaja voi olla omalla kurssillaan myös opiskelijaroolissa ja siten antaa kurssista opintosuorituksen itselleen.

Myös IT-ylläpidossa voi syntyä vaarallisia työyhdistelmiä. Tuleeko esimerkiksi samalla henkilöllä olla sekä oikeus tehdä palomuurirakenteita että kirjautua pääkäyttäjänä



palomuurin suojaamiin palvelimiin? Jos nämä tehtävät on eriytetty kahdelle henkilölle, joutuu uuden palvelun palvelimeen avaava pääkäyttäjä itsensä lisäksi vakuuttamaan myös palomuurin vastuuhenkilön siitä, että käynnistetyn palvelun portin avaaminen Internetiin on varmasti turvallista. Tällä toimenpiteellä vältetään erehdyksiä ja virheitä.

Vaarallisten työtehtävien eriyttämiseen kuuluvat käsitteet staattisesta ja dynaamisesta eriyttämisestä. Jos palvelinten pääkäyttäjien tehtävä ja palomuuariavaukset on eriytetty kokonaan eri henkilöille, kysymys on staattisesta työtehtävien eriyttämisestä. Matkalaskujen teossa on sen sijaan huomioitava, että usein myös matkalaskun hyväksyjällä on omia työmatkoja, joten matkalaskujen tekemistä ei häneltä voida tyystin kieltää. Tällöin riittää, että *omien* matkalaskujen hyväksyminen estetään. Tällöin on kyse dynaamisesta työtehtävien eriyttämisestä; yleisessä tapauksessa henkilö voi sekä tehdä että hyväksyä matkalaskuja, mutta yhdessä ja samassa asiassa (matkalaskussa) henkilö ei voi olla sekä matkustajana että hyväksyjänä.

Organisaation koosta ja toimialasta riippuu, missä määrin vaarallisten työtehtävien eriyttämiseen kiinnitetään huomiota käyttövaltuushallinnassa. Pienessä organisaatiossa kaikkia vaarallisiksi tunnistettuja työyhdistelmiä ei pystytä eriyttämään eri henkilöille, koska mahdolliset henkilöt loppuvat viimeistään lomakauden koittaessa. Tällöin riski joudutaan vain toteamaan ja ottamaan, ja mahdollisesti rakentamaan korvaavia kontrolleja riskin hallitsemiseksi.

## 5.7. Delegointi

Delegointi tarkoittaa käyttäjällä olevien käyttövaltuuksien siirtämistä toiselle käyttäjälle. Delegointi on varsin arkipäiväistä työelämässä; loman tai muun poissaolon ajaksi erilaiset organisaation päivittäiseen toimintaan liittyvät hyväksymis- ja muut valtuudet annetaan varahenkilölle. Organisaatiohierarkiassa tarpeeksi korkealla olevilla on myös taipumus lykätä rutiinejaan, esimerkiksi matkalaskujen tekemisen, sihteereilleen.

Delegointi voi myös liittyä luonnollisten tai juridisten henkilöiden välisiin oikeustoimiin, jolloin käytetään usein käsitettä mandaatti. Yritys voi esimerkiksi ulkoistaa taloushallintonsa tilitoimistolle, jolle annetaan samalla mandaatti hoitaa verottajalle sähköisesti tehtävät kuukausi-ilmoitukset yrityksen puolesta.

Käyttövaltuuksien hallinnan välineet tukevat delegointia vaihtelevalla tavalla. Joissain välineissä käyttövaltuus voidaan delegoida määräajaksi toiselle käyttäjälle, mutta usein delegointi hoidetaan pragmaattisesti antamalla henkilölle ja varahenkilölle molemmille samat valtuudet. Vähimmän käyttövaltuuden periaate jää ehkä silloin toteutumatta, mutta joka tapauksessa järjestely on jäljitettävyyden kannalta parempi kuin se, että henkilö antaa käyttäjätunnuksensa ja salasanasensa varahenkilölleen lomansa ajaksi. Seuraavassa luvussa tutustutaankin jäljitettävyyden käsitteeseen.

## 5.8. Pohdittavaa

- Ryhmiä on pitkään käytetty apuna käyttövaltuuksien hallinnassa esimerkiksi tiedostojärjestelmissä. Miten rooliin perustuvan käyttövaltuuksien hallinnan roolikäsite eroaa ryhmäkäsitteestä?
- Luvussa 5.6 kerrottiin esimerkkinä vaarallisten työtehtävien eriyttämisestä, että matkalaskuohjelma estää käyttäjää hyväksymästä omia matkalaskujaan. Luvussa 3.3 huomautettiin, että organisaation tulee muun muassa päättää, voiko samalla

henkilöllä olla samassa järjestelmässä useita käyttäjätunnuksia. Miten vaarallisten työtehtävien eriyttämisen käy, jos yhdellä käyttäjällä on useita käyttäjätunnuksia?

## 6. Jäljitettävyys ja raportointi

Jäljitettävyys ja raportointi ovat loppukäyttäjälle usein huomaamattomia toimintoja, joilla on tärkeä rooli identiteetin- ja pääsynhallinnan tietoturvallisuutta täydentävinä kontrolleina. Jäljitettävyys ja raportoinnin merkitys vaihtelee toimialoittain; esimerkiksi finanssi- ja terveydenhoitoalalla on omia, toimialasta seuraavia korkeampia erityisvaatimuksia. Esimerkiksi luottokorttimaksujen turvallista vastaanottamista ja käsittelyä koskeva PCI-DSS-standardi asettaa myös jäljitettävyteen liittyviä vaatimuksia.

### 6.1. Jäljitettävyys

Jäljitettävyydellä (accountability) tarkoitetaan luotettavan kirjausketjun (audit trail) muodostamista identiteetin- ja pääsynhallintaan liittyvistä tapahtumista. Kirjausketjun tarkoitus on pystyä tarpeen tullen osoittamaan, kuka käyttäjä on tehnyt tietyn toimenpiteen, ja mihin valtuus tehdä toimenpide on perustunut. Kirjausketjua voidaan käyttää organisaation sisällä ongelmien, vikatilanteiden ja tietoturvaloukkausten tunnistamiseen ja selvittelyyn. Jos palvelusta veloitetaan käytön mukaan, perustuu laskutus usein kirjausketjuun. Kirjausketjua voidaan tarvita myös todistusaineistona – ääritilanteessa tuomioistuimessa – sille, mitä toimenpiteitä tietty käyttäjä on tietojärjestelmässä tehnyt.

Käytännössä keskeistä roolia jäljitettävyyden toteuttamisessa näyttelevät lokitiedot, joita kerätään käyttäjien tunnistamisesta ja heidän käyttövaltuuksiensa myöntämisestä ja käyttämisestä. Jäljitettävyyden varmistamisessa on siis pitkälti kyse siitä, että lokitietojen kerääminen ja eheys varmistetaan osana organisaation muuta lokitietojen hallintaa. Identiteetin- ja pääsynhallinnan lokitiedot ovat käytännössä aina myös henkilötietoja, joten lokitietojen hallinnassa tulee huomioida henkilötietolain ja työnteekijöiden lokitiedoissa myös työelämän tietosuojalain säädökset. Henkilötietolakiin palataan luvussa 9.

Lokitietojen hallinnan lisäksi jäljitettävyys edellyttää kuitenkin myös laajempia toimenpiteitä, joiden laajuus kytkeytyy organisaation riskienhallintaan. Onko esimerkiksi tarpeen pyytää käyttäjältä ensitunnistuksen yhteydessä käsin allekirjoitettu kuittaus, jotta voidaan tarvittaessa osoittaa käyttäjätunnuksen päätyneen oikealle henkilölle? Jos organisaatio kierrättää (re-assign) käyttäjätunnuksia, on myös kyettävä näyttämään, kenelle tosielämän henkilölle käyttäjätunnus on kulloinkin kuulunut.

Ensimmäinen askel parempaa jäljitettävyyttä kohtaan on kuitenkin ryhmätunnuksista luopuminen, joka tarkoittaa henkilökohtaisten käyttäjätunnusten käyttöä kaikkiin toimenpiteisiin. Jäljitettävyys murenee, jos yhden käyttäjätunnuksen takana voi toimia useita tosielämän henkilöitä. Tämä koskee paitsi peruskäyttäjien käyttäjätunnuksia, myös erityisesti pääkäyttäjien käyttäjätunnuksia. Varamiesjärjestelyjen kannalta on toki eduksi, että järjestelmän pääkäyttäjän oikeuksia voi käyttää useita henkilöitä, mutta oikeuksien käyttö tulisi toteuttaa jollain muulla tavalla kuin antamalla pääkäyttäjän (root, administrator) salasana usean henkilön tietoon.

Lisätietoa: Vahti 3/2009. Lokiohje
------------------------------------

### 6.2. Raportointi

Raportointi täydentää jäljitettävyyttä. Siinä missä lokitietojen avulla voidaan muodostaa kuva jo tapahtuneista asioista, raportointivälineiden avulla voidaan tutkia järjestelmässä tällä hetkellä olevien identiteettien ja käyttövaltuuksien tilaa. Raportointivälineiden tulee pystyä tuottamaan ajantasaiset raportit

- käyttäjistä ja heidän rooleistaan
- rooleista ja niihin kytketyistä käyttövaltuuksista
- käyttäjistä ja heidän käyttövaltuuksistaan (edellisten yhdistelmä)
- käyttäjistä, joilla on tietty rooli
- käyttäjistä, joilla on tietyn kohteen käyttövaltuus

Raportointivälineiden pelkkä olemassaolo ei kuitenkaan riitä, vaan organisaation on järjestettävä ja vastuutettava raportointivälineiden säännöllinen käyttö sen selvittämiseksi,

- onko järjestelmissä käyttäjiä, jotka eivät enää ole organisaation palveluksessa
- onko järjestelmissä rooleja, jotka eivät ole enää käytössä
- onko järjestelmissä kohteita ja käyttöoikeuksia, jotka eivät ole enää käytössä
- onko järjestelmässä irrallisia käyttövaltuusmäärittäjiä (ts. liittyen käytöstä poistettuihin suojattaviin kohteisiin tai poistuneisiin rooleihin)
- onko käyttäjiä, joilla on vaarallisia rooli- ja käyttövaltuusyhdistelmiä
- ovatko kohteisiin, rooleihin ja hallintaprosesseihin liittyvät omistajuudet ja niihin liittyvät toimeenpano- ja valvontavastuut hoidossa
- toimivatko hallinnointiprosessit sovitulla tavalla

Raporttien läpikäynti voidaan esimerkiksi kytkeä osaksi organisaation vuosikelloa. Kerran vuodessa vastuuhenkilöt käyvät läpi vastuullaan olevat raportit, tekevät tarvittavat korjaukset ja aktiivisesti hyväksyvät ne tiedot, jotka eivät vaadi korjausta. Identiteetin- ja pääsynhallinnassa tätä kutsutaan attestoinniksi (attest).

## **7. Identiteetin hallinta organisaatiossa**

Edellisissä luvuissa on käsitelty identiteettiä, autentikointia, auktorisointia sekä jäljitettävyyttä ja raportointia. Käsitelyn taso on ollut abstrakti tai suojattavana kohteena on ollut yksi yksittäinen tietojärjestelmä. Tosielämässä tilanne on kuitenkin sellainen, että organisaatiossa on kymmeniä tai satoja tietojärjestelmiä, joissa samalla käyttäjällä on identiteetti ja käyttöoikeuksia. Identiteetin hallinnan tyypillinen haaste on, kuinka identiteettiä hallitaan useista eri tietojärjestelmistä rakentuvassa kokonaisuudessa tarkoituksenmukaisella tavalla.

Tässä luvussa identiteetin hallintaa lähestytään kokonaisarkkitehtuurin näkökulmasta. Luku alkaa kokonaisarkkitehtuuriajattelun esittelyllä. Sen jälkeen syvennyttään identiteetin hallintaa kokonaisarkkitehtuurin kunkin osa-alueen näkökulmasta. Käytännössä identiteetin hallinta-arkkitehtuurin tekninen toteutus tehdään pääosin identiteetin hallintajärjestelmällä, jota käsitellään luvun lopussa.

### **7.1. Kokonaisarkkitehtuuri**

IT-kehityshankkeet ovat usein hankalia organisaation johdolle varsinkin, jos ne nähdään irrallisina teknologiahankkeina, joiden niveltyminen organisaation toimintaan ja tavoitteisiin jää hämäräksi. Identiteetin- ja pääsyn hallinnan kehittämisprojekti ei ole yleensä johdolle kaikkein helpoimmin ymmärrettävä projekti: kalliin hankkeen merkitys organisaation toiminnalle voi jäädä epäselväksi. Toisaalta - kuten tässä luvussa tullaan huomaamaan - identiteetin- ja pääsyn hallinnan projekti lävistää organisaatiota ja sen toimintaa monella tavalla, joten muutoksen läpivieminen edellyttää riittävän korkealta organisaatiosta saatavaa tukea hankkeelle.

Kokonaisarkkitehtuuri (Enterprise Architecture, EA) on viitekehys, joka on kehitetty 1990- ja 2000-luvulla jäsentämään organisaation IT-toimintaa helpommin ymmärrettäväksi ja hallittavaksi kokonaisuudeksi, joka niveltyy organisaation tavoitteisiin. Kokonaisarkkitehtuuri kuvaa, kuinka organisaation elementit – organisaatioyksiköt, ihmiset, toimintaprosessit ja tietojärjestelmät – liittyvät toisiinsa ja toimivat kokonaisuutena. Kokonaisarkkitehtuuri on strategisen johtamisen väline, jonka avulla yhtenäistetään toiminnan kehittämistä.

Kokonaisarkkitehtuuri on tässä valjastettu identiteetin hallinnan arkkitehtuurin kehikoksi, koska kokonaisarkkitehtuurin osa-alueissa nousee esiin myös identiteetin hallinnan arkkitehtuurin keskeiset kysymykset. Jos kokonaisarkkitehtuuri on jo tuttu asia organisaation johdolle, on identiteetin hallinnan kokonaisuuden ymmärtäminen helpompaa kokonaisarkkitehtuurin kautta. Jos organisaatiossa on jo tehty kokonaisarkkitehtuurin mallinnustyötä, saadaan siitä paljon hyödyllistä materiaalia myös identiteetin hallinta-arkkitehtuurin tueksi. Lisäksi kokonaisarkkitehtuurin näkökulma korostaa identiteetin hallinnan näkemistä enemmän johtamiskysymyksenä kuin teknisenä ongelmana.

Tässä alaluvussa esitellään kokonaisarkkitehtuuria vain siinä laajuudessa kuin se on tarpeen identiteetin hallinnan ja kokonaisarkkitehtuurin suhteen ymmärtämiseksi. Kokonaisarkkitehtuurista itsessään on omat kurssinsa ja oppikirjansa, joihin kokonaisarkkitehtuurista, sen eri koulukunnista (mm. TOGAF, Zachman) ja sen kehittämisprosessista laajemmin kiinnostuneet lukijat voivat syventyä.

Kokonaisarkkitehtuuri jaetaan seuraavaan neljään arkkitehtuurin osa-alueeseen, joita seuraavissa luvuissa tarkastellaan identiteetin hallinnan näkökulmasta.

- **Toiminta-arkkitehtuuri** (business architecture) ohjaa arkkitehtuurin muiden osa-alueiden kehittämistä. Kokonaisarkkitehtuurin kehittämisen tarkoituksena on ydintoiminnan tukeminen ja kehittämisen helpottaminen. Kaiken kehittämisen tulee tukea ydintoiminnan strategisia ja taktisia tavoitteita. Toiminta-arkkitehtuuri kuvaa ydintoiminnan organisaatorakenteet, tavoitteet ja prosessit. Näin se myös asettaa tavoitteet ja suuntaviivat arkkitehtuurin muiden osa-alueiden kehittämiselle.
- **Tietoarkkitehtuuri** (information architecture) kuvaa organisaation käyttämät tiedot. Johtamisen näkökulmasta tietojen yhdenmukainen ja yksikäsitteinen ymmärtäminen ja käsittely läpi organisaation on yksi tehokkaan ja virheettömän toiminnan kulmakivistä. Tietoarkkitehtuuri kuvaa tietojen merkityksen, tietovirrat ja tietovarastot.
- **Järjestelmäarkkitehtuuri** (system architecture) kuvaa organisaation järjestelmät ja sen, miten ne tukevat ydintoiminnan tavoitteiden saavuttamista. Järjestelmäarkkitehtuuri kuvaa järjestelmäsalkun, järjestelmien vastuut ja rajaukset sekä liittymät toisiin järjestelmiin.
- **Teknologia-arkkitehtuuri** (IT architecture) kuvaa ne tekniset ratkaisut ja keinot, joiden avulla tuetaan muilla arkkitehtuurin osa-alueilla asetettujen tavoitteiden toteutumista. Teknologia-arkkitehtuurissa kuvataan standardit ja teknologialinjaukset sekä käytettävät työkalut, joiden avulla IT-järjestelmäkokonaisuutta kehitetään.

Lisätietoa: Korkeakoulujen kokonaisarkkitehtuurin käsikirja. Toiminnan ja tietohallinnon kokonaisvaltainen kehittäminen. Helsingin yliopisto, 2009

## 7.2. Toiminta-arkkitehtuuri

Identiteetinhallinta on organisaation tukitoiminto, joka auttaa osaltaan ponnistelemaan kohti organisaation tavoitteiden saavuttamista. Prosessit ovat identiteetinhallinta-arkkitehtuurin toiminta-arkkitehtuuriin kytkevät tekijä. Monesti ydintoiminnan prosesseihin sisältyy tarpeita luoda organisaation toimintaan liittyville henkilölle identiteetti ja kytkeä siihen käyttövaltuuksia.

Organisaation työntekijöille annettavat käyttövaltuudet kytkeytyvät henkilöstöhallinnon prosesseihin. Kun uusi työntekijä palkataan, hänet lisätään organisaation HR-järjestelmään, hänelle suoritetaan ensitunnistus ja luodaan käyttäjätunnus identiteetinhallinta-järjestelmään. Osa työntekijän käyttöoikeuksista voidaan johtaa suoraan HR-järjestelmässä olevista tiedoista, kuten organisaatioyksiköstä ja tehtävänimikkeestä. Lisäksi työntekijä voi saada muita työtehtävien tekemiseen liittyviä käyttöoikeuksia organisaation eri tietojärjestelmiin, jolloin lisäoikeuksille tarvitaan organisaation toimintakäytäntöjen mukaiset hyväksynnit. Kun työntekijän työtehtävät muuttuvat, vanhojen tehtävien hoitoon liittyvät oikeudet poistetaan vähimmän käyttövaltuuden periaatteen mukaisesti. Kun työntekijä poistuu organisaation palveluksesta, hänen käyttöoikeutensa poistetaan ja käyttäjätunnuksensa suljetaan.

Henkilökunnan käyttäjätunnusten hallintaprosessi tuntuu luontevalta, mutta käytännössä siihen kytkeytyy monia kompastuskiviä, jotta HR-järjestelmän tietoja voitaisiin käyttää avuksi identiteettien ylläpitämisessä. Se edellyttävät käytännössä HR-prosessien huolellista suunnittelua ja määrämuotoistamista myös identiteetinhallinnan näkökulmasta.

Henkilöstöhallinto on usein kehittänyt toimintaprosessinsa palvelemaan lähinnä omia tarpeitaan, joihin identiteetinhallinta ei välttämättä kuulu. Seuraavassa on kuvattu tyypillisiä ongelmia

- uusien työsuhteiden vieminen HR-järjestelmään. Uuden työntekijän tiedot tulee olla vietyinä HR-järjestelmään ennen työsuhteen alkua, jotta hänelle voidaan antaa tarvittavat käyttäjätunnukset HR-järjestelmästä saatavan herätteen perusteella heti ensimmäisenä työpäivänä. Joillain toimialoilla tämä saattaa olla hyvinkin haastavaa esimerkiksi tilapäis- ja keikkatyöntekijöiden kohdalla.
- ketjutetut määräaikaisten työsuhteet. Myös uuden määräaikaaisuuden alkaessa uuden työsuhteen tiedot tulee viedä HR-järjestelmään ajoissa. Esimiehillä saattaa olla houkutus sopia työsuhteen jatkamisesta suullisesti ja hoitaa muodollisuudet, kuten uusi työsopimus, joskus myöhemmin.
- henkilökuntaan rinnastuvat käyttäjät. Monessa organisaatiossa on henkilöitä, jotka eivät ole työsuhteessa organisaatioon (ja siten organisaation HR-järjestelmässä), mutta joilla kuitenkin on henkilökuntaan rinnastuvia käyttöoikeuksia tietojärjestelmissä. Tällaisia henkilöitä ovat esimerkiksi ulkoistetut työntekijät ja vuokratyövoima, kuten vahtimestarit, siivoojat, konsultit tai siviilipalvelusmiehet. Myös näiden henkilöiden identiteetit tulee pystyä hallitsemaan luotettavasti, vaikka heidän palvelussuhteensa alkamisesta ja päättymisestä ei koskaan tule merkintää HR-järjestelmään. Usein ensimmäinen ratkaistava kysymys on, kuka organisaatiossa ottaa vastatakseen tällaisten henkilöiden identiteetinhallinta-prosessin suunnittelusta ja toteutuksesta.

Henkilökunnan ja heihin rinnastuvien muiden **sisäisten käyttäjien** vastakohtana organisaatiolla on usein myös **ulkoisia käyttäjiä**, jotka toimialasta riippuen voivat olla esimerkiksi asiakkaita, alihankkijoita, potilaita tai opiskelijoita. Sisäisten ja ulkoisten käyttäjien käsitteiden ero on lähinnä käyttövaltuuksien laajuudessa; työsuhteessa tai siihen rinnastuvassa toimeksiantosuhteessa olevilla henkilöillä on yleensä laajemmat käyttövaltuudet tietojärjestelmissä kuin ulkoisilla käyttäjillä. Usein ulkoiset käyttäjät eivät myöskään pääse organisaation sisäverkkoon.

Myös ulkoisten käyttäjien identiteettiensä ja käyttövaltuuksiensa ylläpito niveltyy läheisesti heitä koskeviin toimintaprosesseihin, kuten asiakkuudenhallintaan tai toimittajienhallintaprosessiin. Esimerkiksi yrityksen asiakkaaksi tuleville yrityksille tai yksityishenkilöille annetaan tarvittavat käyttäjätunnukset ja käyttöoikeudet yrityksen extranet-palveluun samalla, kun asiakkaan kanssa solmitaan tarpeelliset asiakassopimukset. Kun asiakkuus päättyy, myös käyttäjätunnukset suljetaan. Ulkoisten käyttäjien identiteetinhallinta tarvitsee siis suunnitella osana mainittua prosessia yhteistyössä prosessista vastaavan organisaatioyksikön kanssa niin, että organisaation toiminnan tavoitteet tulevat huomioituksi kokonaisuutena.

### 7.3. Tietoarkkitehtuuri

Tyypillisesti samaa henkilöä koskevia tietoja on organisaatiossa monessa eri tietojärjestelmässä. Esimerkiksi työntekijöitä koskevaa tietoa on kaikissa järjestelmissä, joihin työntekijä kirjautuu henkilökohtaisella käyttäjätunnuksella, kuten työasemaympäristössä, Intranetissä jne. Lisäksi työntekijän tietoja on tyypillisesti HR-järjestelmissä, kulunhallintajärjestelmässä, puhelinvaihteessa ja niin edelleen. Myös ulkoisten käyttäjien tietoja on useassa tietojärjestelmässä.

Organisaatiossa tehdään moninkertaista työtä, jos samojen henkilöiden samoja tietoja ylläpidetään useassa rinnakkaisessa, toisistaan tietämättömässä tietojärjestelmässä. Jos tietojen ylläpitoprosessi ei ole aukoton, saattaa muuttuneen tiedon päivittäminen lisäksi unohtua johonkin sen rinnakkaisista instansseista, jolloin tiedon eheys menetetään.

Master data management<sup>9</sup> (MDM) –käsitteellä tarkoitetaan prosessia ja välineitä, jolla pyritään karsimaan saman tiedon päällekkäisten instanssien hallintaa organisaatiossa. Master data management muodostaa keskeisen osan identiteetinhallinnan tietoarkkitehtuuria. Jokaiselle identiteettiin liittyvälle attribuutille määritellään **autoratiivinen lähde**: tietojärjestelmä, josta attribuutin arvo valutetaan muihin järjestelmiin. Tämän jälkeen toiminta organisoidaan siten, että tietoa ylläpidetään ja tiedon muutokset tehdään vain tiedon autoratiiviseen lähteeseen. Käsitteellisesti kysymys on samasta asiasta kuin tietokantojen normalisoinnissa.

Autoratiivisten lähteiden valinta edellyttää organisaation toiminnan tuntemusta, jotta pystytään ottamaan näkemys autoratiivisen lähteen luontevimmasta sijainnista. Joitain esimerkkejä mahdolliseksi autoratiiviseksi lähteestä on allaolevassa taulukossa:

Attribuutti	Esimerkki autoratiivisesta lähteestä
Työntekijän nimi ja työntekijänumero	HR-järjestelmä
Työntekijän organisaatioyksikkö	HR-järjestelmä
Käyttäjätunnus ja salasana	Identiteetinhallintajärjestelmä (IdM)
Työntekijän puhelinnumero	Puhelinvaihde
Työntekijän sähköpostiosoite	Sähköpostipalvelin

Lisäksi yleensä on tarve korottaa joku autoratiivisista järjestelmistä **perusrekisteriksi**: keskitetyksi pisteeksi, josta uudet identiteetit tulevat organisaatioon. Tämä tarkoittaa, että uusi identiteetti tulee identiteetinhallintaan aina siten, että identiteetti lisätään ensi perusrekisteriin, mikä liipaisee identiteetin perustamisen myös muihin järjestelmiin. Vastaavasti identiteetti suljetaan, kun se suljetaan tai poistetaan perusrekisterissä. Teknisestä näkökulmasta voidaan ajatella, että autoratiivinen lähde ”omistaa” identiteetinhallintajärjestelmässä olevan attribuutin ja perusrekisteri puolestaan ”omistaa” identiteetin (vaikka identiteetin eri attribuutit voivatkin olla eri autoratiivisen lähteen omistuksessa).

Perusrekistereitä voi olla useita. Jos organisaatiossa on erityyppisiä identiteettejä, niillä on usein eri perusrekisterit. Esimerkiksi henkilökunnan identiteeteille luonteva kandidaatti perusrekisteriksi on HR-järjestelmä, jossa organisaation voimassaolevat työsuhteet voidaan ajatella olevan parhaiten ajan tasalla. Vastaavasti asiakkaiden perusrekisteri voisi olla asiakashallintajärjestelmä, potilaiden perusrekisteri potilastietojärjestelmä ja opiskelijoiden perusrekisteri opiskelijarekisteri. Edellä luvussa 7.2 viitattiin myös tarpeeseen hallita henkilökuntaan rinnastuvien käyttäjien identiteettejä; myös heidän identiteettinsä on syytä hallita organisaatiossa keskitetysti.

Perusrekisterien valinnan yhteydessä tulee myös ratkaistavaksi erikoistilanteet, joissa sama henkilö esiintyy useita kertoja samassa tai eri perusrekistereissä. Työntekijällä voi olla

<sup>9</sup> Master data management –käsitteelle ei ole vakiintunut suomenkielistä termiä. Mm. perustiedon hallinta –termiä on ehdotettu.



esimerkiksi useita samanaikaisia työsuhteita organisaatiossa, tai samalla konsultilla voi olla useita yhtäaikaista toimeksiantoja organisaatiossa. Korkeakouluissa puolestaan on tavallista, että sama henkilö on sekä opiskelijana että työntekijänä, jolloin hänellä on tietue sekä opiskelija- että henkilökuntarekistereissä. Tietoarkkitehtuurissa tulee tällöin ottaa kantaa siihen, sallitaanko rinnakkaisten identiteettien syntyminen samalle tosielämän henkilölle, ja millaisia seurannaisvaikutuksia sillä on. Vaarallisten työyhdistemien eriyttäminen saattaa esimerkiksi käydä hankalaksi tai mahdottomaksi, jos tietojärjestelmät eivät pysty päättämään kahden eri käyttäjätunnuksen kuulumista samalle tosielämän henkilölle. Rinnakkaisten identiteettien sallimisen vaihtoehtona on ylläpitää henkilölle vain yhtä identiteettiä, johon liittyy useita rooleja.

Attribuutti	Autoratiivinen lähde	Kohdejärjestelmät			
		Windows AD	Matkalaskujen hallinta	Intranet	Sähköposti-palvelin
Henkilönumero	HR	X	X		
Nimi	HR	X	X	X	X
Salasana	Windows AD	X	X	X	X
Mail-osoite	Sähköposti-palvelin	X	X		
...					

Kun tietovirrat, autoratiiviset lähteet ja perusrekisterit on selvillä, voidaan tietovirrat koota yhteen taulukoksi. Kullekin attribuutille merkitään taulukkoon autoratiivinen lähde sekä ne kohdejärjestelmät, joihin attribuutin arvot valutetaan autoratiivisesta lähteestä. Käytännössä valuttamisesta huolehtii organisaation identiteetinhallintajärjestelmä, johon syvennyttään tuonnempana luvussa 7.7. Taulukko on varsin tehokas väline kokonaiskuvan saamiseksi tietovirroista.

Tietovirtojen määrittelyn lisäksi tietoarkkitehtuuriin liittyy sopimukset tiedon syntaksista ja semantiikasta. On tyypillistä, että eri organisaatioyksiköissä on erilainen näkemys attribuuttien arvoihin ja mahdollisten arvojen merkitykseen. Tietoarkkitehtuurissa syntaksi ja semantiikka tulee yhtenäistää, tai vaihtoehtoisesti suorittaa attribuuttien muunnosajoja samalla, kun attribuuttien arvoja valutetaan autoratiivisesta lähteestä muihin järjestelmiin. Esimerkkejä sovittelua kaipaavista attribuuttien semantiikasta ovat

- Henkilöstöhallinnon mielestä työntekijän tunnusmerkki on voimassaoleva työsuhde, esimerkiksi tietohallinto saattaa pitää myös henkilökuntaan rinnastuvia käyttäjiä työntekijöinä.
- Henkilöstöhallinnon, taloushallinnon ja muiden tukipalveluiden näkemys organisaatorakenteesta, kustannuspaikka- tai projektikoodeista ja niiden esittämisestä attribuuttina saattaa poiketa toisistaan.
- Henkilöstöhallinnon mielestä perhevapaalla, armeijassa tai pitkällä sairauslomalla oleva henkilö on edelleen työsuhteessa, mutta tietohallinnon käsityksen mukaan hänen käyttäjätunnuksensa tulee sulkea.

Autoratiivisten lähteiden ja perusrekisterien kiinnittäminen ja tiedon syntaksin ja semantiikan määrittäminen ovat usein monimutkaisia asioita, joiden sopimista varten tarvitaan asiantuntemusta kaikista kyseisiä tietoja tuottavista ja käyttävistä organisaatioista. Missään tapauksessa tehtävää ei saa jättää pelkästään tietotekniikan asiantuntijoiden harteille, vaikka tietojen valuttaminen autoratiivisesta lähteestä muihin järjestelmiin hoidetaankin käytännössä teknisen välineen avulla.

#### **7.4. Järjestelmäarkkitehtuuri**

Identiteetinhallinnan järjestelmäarkkitehtuuri ottaa kantaa siihen, mitkä organisaation järjestelmät otetaan identiteetinhallinnan piiriin. Ideaalitulanteessa kaikki organisaation järjestelmät olisivat organisaation keskitetyn identiteetinhallinnan piirissä. Käytännössä ideaaliin kuitenkin päästään harvoin eikä siihen pyrkiminen ole edes tarkoituksenmukaista, koska jokaisen integraation rakentaminen ja ylläpito maksaa, ja järjestelmän rajapinnoista riippuen integraatio voi pahimmillaan olla työlästäkin. Integraation hankaluutta voi esimerkiksi lisätä järjestelmän ostaminen palveluna (Software as a Service, SaaS), jolloin järjestelmä sijaitsee alihankkijan ympäristössä.

Pragmaattinen lähtökohta on käydä organisaation tietojärjestelmät läpi ja käyttää harkintaa siitä, kannattaako se integroida organisaation keskitettyyn identiteetinhallintaan. Perusrekistereinä ja autoratiivisina lähteinä käytettävät järjestelmät on luonnollisesti kytkettävä identiteetinhallintajärjestelmään. Myös sellaiset palvelut, joissa sulkematta unohtuneet tunnukset aiheuttavat suurimmat tietoturvariskit (esim. henkilökunnan VPN-etäyhteydet), kannattaa ottaa keskitetyn identiteetinhallinnan piiriin. Muiden järjestelmien kytkeminen identiteetinhallintajärjestelmään kannattaa aloittaa suurimman käyttäjämäärän ja käyttövolyymin palveluista. Pienemmissä järjestelmissä myös puoliautomaattinen kytkentä saattaa riittää; identiteetinhallintajärjestelmä saattaa esimerkiksi lähettää sähköpostiviestin ("tiketin") järjestelmän pääkäyttäjälle havaittuaan tarpeen tunnuksen avaamiseen tai sulkemiseen.

On syytä huomata, että identiteetinhallinta ja sen mahdollisuudet pitää nähdä laajemmin kuin pelkkänä käyttäjätunnushallintana. Henkilöillä on identiteettejä myös sellaisissa palveluissa, joissa heillä ei ole käyttäjätunnuksia ja joihin he eivät "kirjaudu sisään" sanan totutussa merkityksessä. Tällaisia palveluita ovat esimerkiksi kulunhallintajärjestelmät, joissa ajantasaiset identiteetit ovat kuitenkin tärkeitä toimitilaturvallisuuden vuoksi, mutta "sisäänkirjautuminen" tapahtuu esimerkiksi näyttämällä kulkukorttia ovenssa olevalle kortinlukijalle. Sähköisten kulunhallintajärjestelmien rinnalla on edelleen fyysisiä avaimia, joiden haltijoista pidetään niin ikään kirjaa. Organisaation puhelinvaihe käsittelee myös ainakin henkilökuntaan kuuluvien henkilöiden identiteettejä, jotta puhelut saadaan yhdistettyä ja laskutettua oikein. Myös näiden järjestelmien ottaminen keskitetyn identiteetinhallinnan piiriin on syytä selvittää.

#### **7.5. Teknologia-arkkitehtuuri**

Identiteetin- ja pääsynhallinnan teknologia-arkkitehtuuri kuvaa ne välineet, standardit ja teknologiat, joilla organisaation identiteetin- ja pääsynhallinta toteutetaan. Teknologia-arkkitehtuuri esimerkiksi kuvaa, minkälaisia teknisiä rajapintoja järjestelmät voivat käyttää asioidessaan organisaation identiteetinhallintajärjestelmän kanssa. Uusia tietojärjestelmiä hankittaessa tulee varmistaa, että järjestelmät tukevat organisaatiossa käytössä olevaa teknologia-arkkitehtuuria.

Organisaation identiteetin- ja pääsynhallinnan teknologia-arkkitehtuuriin voi esimerkiksi sisältyä

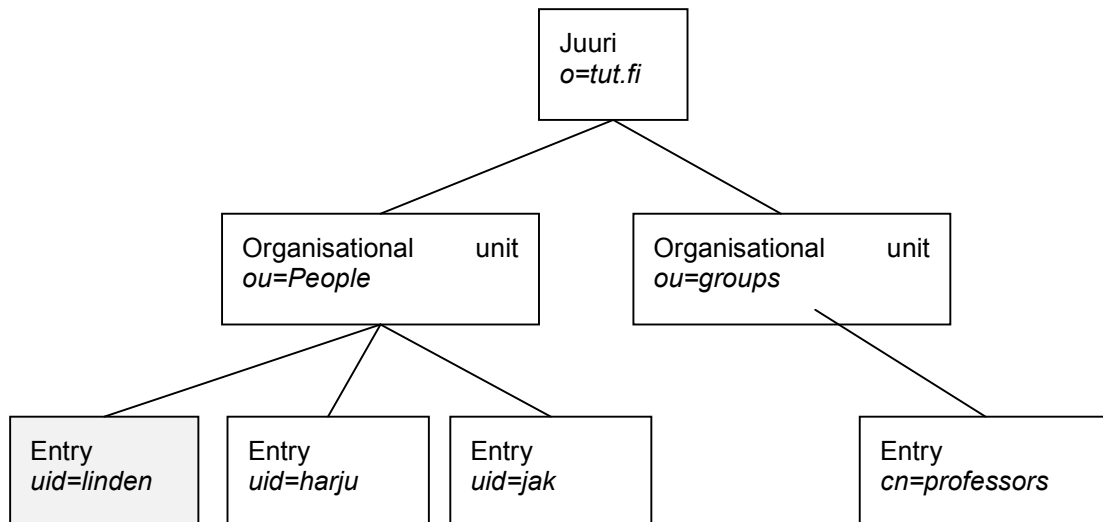
- LDAP-hakemiston käyttö palveluille tarjottavana rajapintana organisaation käyttäjätietoihin, joka mahdollistaa myös käyttäjän tunnistuksen. LDAP-hakemistosta kerrotaan lisää alla.
- Standardit, teknologiat tai tuotteet, joiden avulla käyttäjien identiteetit voidaan perustaa (provisioida) tai sulkea (deprovisioida) niissä järjestelmissä, jotka nojaavat organisaation keskitettyyn identiteetinhallintaan, mutta eivät tue yllämainittua LDAP-hakemistoa. Provisiointiin ja deprovisiointiin palataan luvussa 7.7.
- Standardit, teknologiat tai tuotteet, joita organisaatiossa käytetään kertakirjautumisen työasemaympäristössä (esim. ESSO-tuote tai Windows-toimialuekirjautuminen) tai Web-palveluissa (esimerkiksi web proxy). Kertakirjautumista käsiteltiin luvussa 4.7.
- Standardit, teknologiat tai tuotteet, joita organisaatiossa käytetään identiteetin- ja pääsynhallintaan organisaation ulkopuolisissa palveluissa. Federoituun identiteetinhallintaan palataan luvussa 8.

Usein teknologia-arkkitehtuuriin sisältyy ainakin LDAP-hakemisto, joten siihen paneudutaan seuraavassa alaluvussa hieman syvemmin.

## 7.6. LDAP-hakemisto

LDAP-hakemisto (Light-weight Directory Access Protocol) on laajasti käytetty standardi hakemistopalvelu identiteettitiedon tarjoamiseen sitä tarvitseville palveluille. Tavallisista tietokannoista hakemisto eroaa ennen kaikkea siinä, että se on optimoitu hakemiseen – hakemiston tietoja luetaan paljon mutta kirjoitetaan harvemmin. LDAP-hakemistosta voidaan hakea hakukriteerin täyttäviä tietueita, esimerkiksi tietyn käyttäjätunnuksen haltijan attribuutteja, joiden nimeämiseen käytettävät skeemat esiteltiin edellä luvussa 3.2. Käyttäjätietueeseen liittyy myös käyttäjän salasana, joten käyttäjä voidaan autentikoida LDAP-hakemistoa vasten.

LDAP-hakemistoon talletettu tieto on organisoitu hierarkiaksi, jossa voi olla useita tasoja. Kuvan esimerkissä (Kuva 16) juurisolmun alla on kaksi alisolmua, toinen käyttäjille (ou=people) ja toinen ryhmille (ou=groups). Varsinaiset käyttäjätietueet on koottu käyttäjäsolmun alle (uid=<käyttäjätunnus>). Solmujen nimeksi (RDN, Relative Distinguished Name, kuvassa kursiivilla) valitaan tietueen attribuutti, jonka arvo on yksikäsitteinen sisärsolmujensa joukossa.



**Kuva 16. Esimerkki LDAP-hakemistosta**

Jokainen LDAP-hakemiston solmu voidaan osoittaa sen DN-nimellä (Distinguished Name), joka koostuu solmun ja sen vanhempien RDN-arvoista. Esimerkiksi kuvan harmaan solmun DN on *uid=linden, ou=People, o=tut.fi*.

LDAP-määrittäjäperhe määrittelee myös kuljetuskerroksen (TCP) päällä ajettavan request/response-protokollan, jolla asiakasohjelmat voivat asioida LDAP-hakemiston kanssa. Protokollan tärkeimmät viestit ovat *search*, jolla haetaan tietoja hakemistosta ja *bind*, jonka avulla hakemisto voi autentikoida käyttäjän. Koska LDAP-protokolla itsessään ei huolehdi tiedonsiirron turvallisuudesta, tunneloidaan se yleensä TLS/SSL-protokollan yli. Koska LDAP-hakemistot sisältävät henkilötietoja, niihin ei yleensä sallita liikennettä sisäverkon ulkopuolelta. Ohessa (Kuva 17) on esimerkki LDAP-hausta ja sen tuloksena löytyneistä attribuuteista.

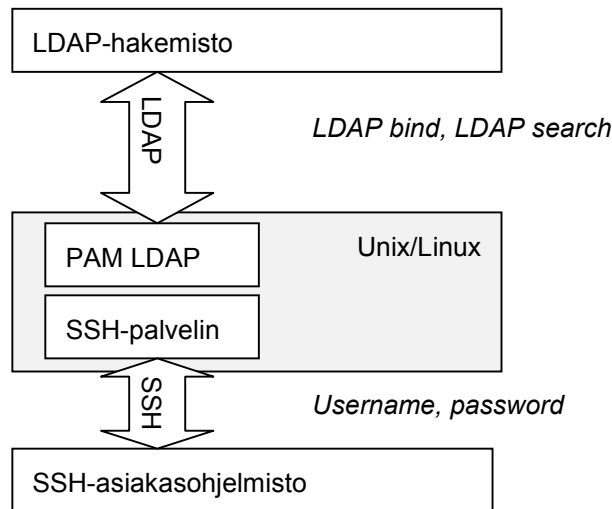
```

linden@mustatilhi ~ $ ldapsearch -h ldap.tut.fi -b uid=linden,ou=People,o=tut.fi objectClass=*
dn: uid=linden,ou=People,o=tut.fi
objectClass: eduPerson
objectClass: funetEduPerson
objectClass: inetOrgPerson
mail: mikael.linden@tut.fi
uid: linden
sn: Linden
cn: Mikael Linden
givenName: Mikael Juhani
....
  
```

**Kuva 17. Esimerkki LDAP-clientista ja anonyymien (autentikoimattoman) LDAP-haun tuloksista.**

Esimerkiksi sähköpostiasiakasohjelmiston voi konfiguroida käyttämään LDAP-hakemistoa osoitekirjanaan, mutta tyypillinen käyttötilanne on, että käyttäjätunnistusta edellyttävä palvelin konfiguroidaan tunnistamaan käyttäjä LDAP-hakemistoa vasten. Oheisessa kuvassa (Kuva 18) on esitetty Unix/Linux-palvelin, johon avataan komentorivi-istunto SSH Secure Shell -yhteyden ylitse. Käyttäjä syöttää käyttäjätunnuksensa ja salasansa osana SSH-istunnon muodostamista. SSH-palvelin on konfiguroitu käyttämään Unix/Linux-käyttöjärjestelmän PAM-rajapintaa (pluggable authentication module) salasanan tarkistamiseen LDAP-hakemistosta. PAM LDAP -moduuli rakentaa käyttäjätunnuksen ja salasanan avulla tarvittavat LDAP bind ja search -pyynnöt. Jos salasana oli oikein, LDAP-hakemisto palauttaa SSH-palvelimelle komentorivi-istunnon

muodostamiseen tarvittavat tiedot, kuten käyttäjän ryhmätiedot, komentotulkin ja kotihakemiston sijainnin.



**Kuva 18. Unix/Linux-palvelin, joka autentikoi käyttäjän LDAP-hakemistoa vasten.**

Saatavilla on runsaasti avoimen lähdekoodin LDAP-hakemistoja ja kaupallisia tuoteperheitä, joihin sisältyy LDAP-hakemisto. Muun muassa Windows-toimialueen ytimen muodostava Active Directory on LDAP-hakemisto.

## 7.7. Identiteetinhallintajärjestelmä

Edellisissä alaluvuissa on esitelty identiteetin- ja pääsynhallinnan kokonaisarkkitehtuuria toiminnan, tiedon, tietojärjestelmien ja teknologian näkökulmista. Alalukujen tarkoitus oli korostaa, että identiteetinhallinnan kehittämisprojektiin liittyy monenlaisia määrittely-, suunnittelu- ja johtamisasioita, eikä identiteetinhallinnan kehittämisprojektia saa siksi ajatella pelkästään teknisenä järjestelmähankkeena. Tässä luvussa tutustutaan lopulta identiteetinhallinnan tietojärjestelmään ja sen ominaisuuksiin.

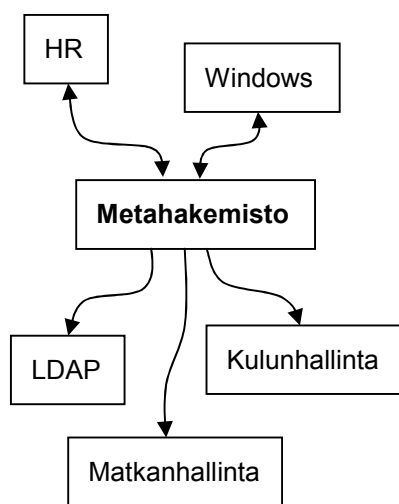
Identiteetinhallintajärjestelmän (IdM-järjestelmä) voi toki toteuttaa kotikutoisesti tietokannalla, LDAP-hakemistolla ja sen ympärille ohjelmoiduilla skripteillä jne. Pienessä<sup>10</sup> ja yksinkertaisessa organisaatiossa tämä onkin harkinnanarvoinen vaihtoehto. 2000-luvulla tarjolle on myös tullut valmiita (pääasiassa kaupallisia) identiteetinhallintatuotteita, joiden tyypillisiin ominaisuuksiin luodaan tässä katsaus. Yksittäisiä tuotteita ja niiden vertailua ei tässä tehdä<sup>11</sup>.

**Metahakemisto** (metadirectory) on identiteetinhallintajärjestelmän ydin. Metahakemisto on ”hakemistojen hakemisto”, joka on konfiguroitu synkronoimaan organisaation eri käyttäjätietokantoja toisiinsa tietoarkkitehtuurin (luku 7.3) mukaisesti (Kuva 19a). Kun metahakemisto havaitsee, että perusrekisteriin on syntynyt uusi identiteetti, metahakemisto perustaa eli **provisioi** identiteetin muiden tietojärjestelmien (kohdejärjestelmät) käyttäjätietokantoihin, ja kalustaa perustetut identiteetit käyttäjän perustiedoilla ja hänelle

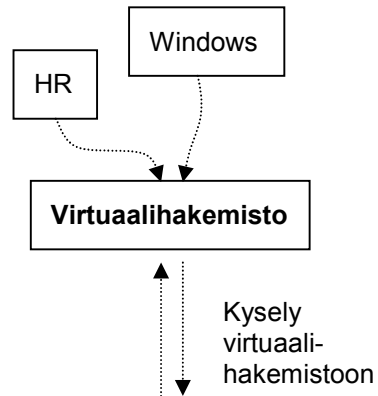
<sup>10</sup> Joidenkin konsulttien mielestä kaupallisen identiteetinhallintajärjestelmän käyttöönotto ei kannata alle 500 työntekijän organisaatiossa.

<sup>11</sup> Saatavilla on kaupallisten tutkimuslaitosten tekemiä identiteetinhallintajärjestelmien säännöllisiä vertailuja, mm. Gartner: Magic Quadrant for User Provisioning.

kuuluvilla perusvaltuuksilla. Kun metahakemisto havaitsee, että identiteetin jonkun attribuutin arvo on muuttunut autoratiivisessa lähteessä, metahakemisto huolehtii, että muuttunut attribuutin arvo valutetaan myös kohdejärjestelmiin. Kun käyttäjän identiteetti perusrekisterissä suljetaan (esimerkiksi työntekijän työsuhte kirjataan päättyneeksi), metahakemisto sulkee eli **deprovisioi** käyttäjän identiteetit kohdejärjestelmissä. Tämä voi tarkoittaa esimerkiksi, että käyttäjän tietue poistetaan kokonaan (esim. kulunhallintajärjestelmästä) tai että käyttäjän tiedot ja tiedostot jäävät ennalleen (esim. Windows-toimialueessa), mutta käyttäjätili asetetaan tilaan, jossa kirjautuminen on estetty. Suljetut tilit poistetaan myöhemmin siivousajossa organisaation toimintakäytännön mukaisesti.



(a) Metahakemisto



(b) Virtuaalihakemisto

**Kuva 19. Metahakemisto (a) valuttaa muuttuneita tietoja autoratiivisista lähteistä kohdejärjestelmiin (nuolen suunta) jatkuvasti tai ajastetuilla eräajoilla. Virtuaalihakemisto (b) puolestaan selvittää tiedon ajantasaisen arvon lähdejärjestelmästä juuri sillä hetkellä, kun joku kohdejärjestelmä kysyy sitä.**

Kopioidessaan tietoja perusrekistereistä ja autoratiivisista lähteistä kohdejärjestelmiin metahakemisto tekee tiedolle tarvittavat muunnokset, jos esimerkiksi attribuuttien nimeäminen tai syntaksi ja semantiikka eivät ole samanlaiset lähde- ja kohdejärjestelmissä. Tyypillisesti metahakemisto huolehtii myös salasanasynkronoinnista: käyttäjä ohjeistetaan vaihtamaan salasansansa yhdessä keskitetyssä paikassa (esimerkiksi IdM-järjestelmän tarkoitusta varten tarjoamalla WWW-sivulla), ja metahakemisto huolehtii vaihdetun salasanan viemisestä kaikkiin kohdejärjestelmiin. Vaikka organisaatiossa ei olisi käytössä kertakirjautumista, saadaan näin toteutettua yhden salasanan periaate. Myös organisaation IT-tuella on käyttöliittymä, josta se voi uusien käyttäjän unohtaman salasanan.

Metahakemisto siis lukee lähdejärjestelmien ja kirjoittaa kohdejärjestelmien käyttäjätietokantoja järjestelmien sovelluslogiikan ohi. Tätä varten metahakemiston tulee liittyä suoraan järjestelmien tietokantoihin. Liitynnän suorittavia ohjelmistoja kutsutaan **konnektoreiksi** (connector). Vaikka olemassa on joitain standardeja provisiointiprotokollia (esim. Simple Provisioning Markup Language, SPML ja Simple Cloud Identity Management, SCIM), sisältävät identiteetinhallintajärjestelmätuotteet yleensä suuren joukon konnektoreita, joiden avulla identiteettejä voidaan provisioida ja deprovisioida eri tuotteiden käyttäjätietokantaan.

**Virtuaalihakemisto** (Virtual directory) esitetään usein vaihtoehtoisena ja jossain määrin korvaavana ratkaisuna metahakemistolle. Siinä missä metahakemisto suorittaa tietojen kopiointia lähdejärjestelmistä kohdejärjestelmiin, virtuaalihakemisto (Kuva 19b) tyytyy pelkästään pitämään kirjaa autoratiivisen tiedon sisältävistä lähdejärjestelmistä. Kun virtuaalihakemistoon tehdään haku (esimerkiksi normaaliin tapaan LDAP-protokollan avulla), virtuaalihakemisto käy noutamassa tarvittavat tiedot lennossa niiden autoratiivisista lähteistä, ja muodostaa hakuun vastauksen häiritsemättä kysyjää yksityiskohdilla autoratiivisen tiedon sijainnista.

Jos käyttäjän rooli tai käyttövaltuus palvelussa voidaan johtaa suoraan lähdejärjestelmistä saatavan tiedon perusteella, pystyy metahakemisto antamaan käyttäjälle kuuluvan roolin tai käyttövaltuuden suoraan kohdejärjestelmään. Jos esimerkiksi jokaiselle työntekijälle kuuluu automaattisesti oikeus työasemakirjautumiseen ja sähköpostilaatikkoon sekä matkalaskujen tekemiseen, voidaan (ja usein myös kannattaa) työasematunnus (asiaankuuluvine käyttäjäryhmineen), sähköpostilaatikko sekä oikeus käyttää matkahallintajärjestelmään matkustajaroolissa perustaa heille automaattisesti.

Usein kuitenkin organisaation toimintakäytännöt edellyttävät, että roolin tai käyttövaltuuden myöntämisen käyttäjälle hyväksyy hänen esimiehensä, kyseisen järjestelmän omistaja tai muu vastaava henkilö. Perinteisessä toimintamallissa käyttövaltuuksien anominen on tapahtunut paperilomakkeella, jonka käyttövaltuuden hakija täyttää ja allekirjoittaa ja johon hän sitten hakee tarpeelliset hyväksynnot organisaatiossa. Sen jälkeen käyttövaltuus on toteutettu, eli pääkäyttäjä on käynyt luomassa henkilölle käyttövaltuuden järjestelmään. Lopuksi lomake on arkistoitu mappiin jäljitettävyyden toteutumiseksi. Identiteetinhallintajärjestelmä sisältää usein tämän prosessin sähköistämisen mahdollistavan välineen, jota kutsutaan **työnkuluksi** (workflow). Käyttövaltuuden hakija ei täytäkään paperista lomaketta, vaan kirjautuu identiteetinhallintajärjestelmän työnkulkuvälineeseen, yksilöi hakemansa roolin tai käyttövaltuuden, perustelee hakemuksensa sanallisesti WWW-lomakkeella ja lähettää lomakkeen eteenpäin. Sähköinen lomake kiertää sille määritellyn hyväksymisketjun, jossa hyväksynnot annetaan niin ikään sähköisesti. Lopuksi rooli tai valtuus toteutetaan ja hakemus arkistoidaan myöhempiä raportointitarpeita varten. Toteuttaminen voi tapahtua joko täysin automaattisesti, jolloin metahakemisto huolehtii roolin tai valtuuden syntymisestä kohdejärjestelmään, tai toteuttaminen voi edellyttää ihmisen väliintuloa. Jälkimmäisessä tapauksessa työnkulku synnyttää esimerkiksi tapahtuman (tiketin), johon järjestelmän pääkäyttäjä reagoi. Työnkulkujärjestelmän käytön voi laajentaa edelleen koskemaan myös materiaalisia hakemuksia, esimerkiksi matkapuhelinta tai etätyöyhteyttä.

Tyypillisesti identiteetinhallintajärjestelmät sisältävät myös välineet organisaation edellyttämien, käyttäjiä, käyttäjien rooleja ja käyttövaltuuksia koskevien **raporttien tuottamiseen** (luku 6.2) identiteetinhallintajärjestelmän piirissä olevista tiedoista. Esimiehet voidaan lisäksi esimerkiksi pakottaa aktiivisesti vahvistamaan vuosittain, että heidän aikaisemmin myöntämänsä käyttövaltuudet ovat edelleen voimassa (attestointi). Näin pyritään vähimmän käyttövaltuuden periaatteen mukaisesti siivoamaan pois henkilöille kertyneet, tarpeettomiksi käyneet käyttövaltuudet.

Luvussa 5.3 käsiteltiin rooliin perustuvaa käyttövaltuuksien hallintaa, joka on muuttunut organisaatioiden identiteetin ja käyttövaltuuksien hallinnan valtavirraksi. Identiteetin-hallintatuotteisiin on kehitetty toiminnallisuuksia, joilla pyritään tukemaan organisaation **roolien elinkaaren hallintaa**. Ennen kuin rooli voidaan antaa kenellekään käyttäjälle, täytyy rooli perustaa, määritellä ja sille nimetä omistaja. Roolin elinkaaren kuuluu lisäksi

roolien antaminen ja poistaminen käyttäjiltä, rooliin liittyvät muutokset, raportit ja roolin poistaminen.

Vaikka identiteetinhallintajärjestelmien toteuttajat ponnistelevatkin järjestelmiensä helppokäyttöisyyden kehittämiseksi, identiteetinhallintajärjestelmien käyttöönotto on usein varsin työläs projekti, jossa ensin suunnitellaan organisaation identiteetinhallinta-arkkitehtuuri, ja sen jälkeen identiteetinhallintajärjestelmä rakennetaan identiteetinhallinta-arkkitehtuurin mukaiseksi. Eri lähteistä saatavien tietojen mukaan identiteetinhallinta-projektin kuluista 25-30% muodostuu käytettävän identiteetinhallintajärjestelmän tuotelisensseistä, ja loput määrittelyyn, suunnitteluun, toteutukseen ja testaukseen kuluva työstä.

## **7.8. Pohdittavaa**

- Kenelle organisaation identiteetinhallinta-arkkitehtuurin suunnitteluvastuu kuuluu? Tietohallinnolle? Henkilöstöhallinnolle? Jollekin muulle?
- Tietoarkkitehtuuriin liittyen todettiin, että organisaatiossa saattaa olla useita perusrekistereitä, ja sama tosielämän henkilö voi esiintyä useassa perusrekisterissä. Sama henkilö esimerkiksi voi olla sekä korkeakoulun opiskelija- että henkilökuntarekisterissä. Miten tällainen tilanne voidaan käytännössä tunnistaa? Jääkö jotain ongelmia vielä ratkaisematta?
- Identiteetinhallintajärjestelmän itsensä tietoturvallisuudesta huolehtiminen on mitä ilmeisimmin tärkeää. Minkälaisia luottamuksellisuus-, eheys- ja saatavuusvaatimuksia identiteetinhallintajärjestelmään kohdistuu? Minkälaisia toimenpiteitä identiteetinhallintajärjestelmän suojaamiseksi voidaan tehdä?

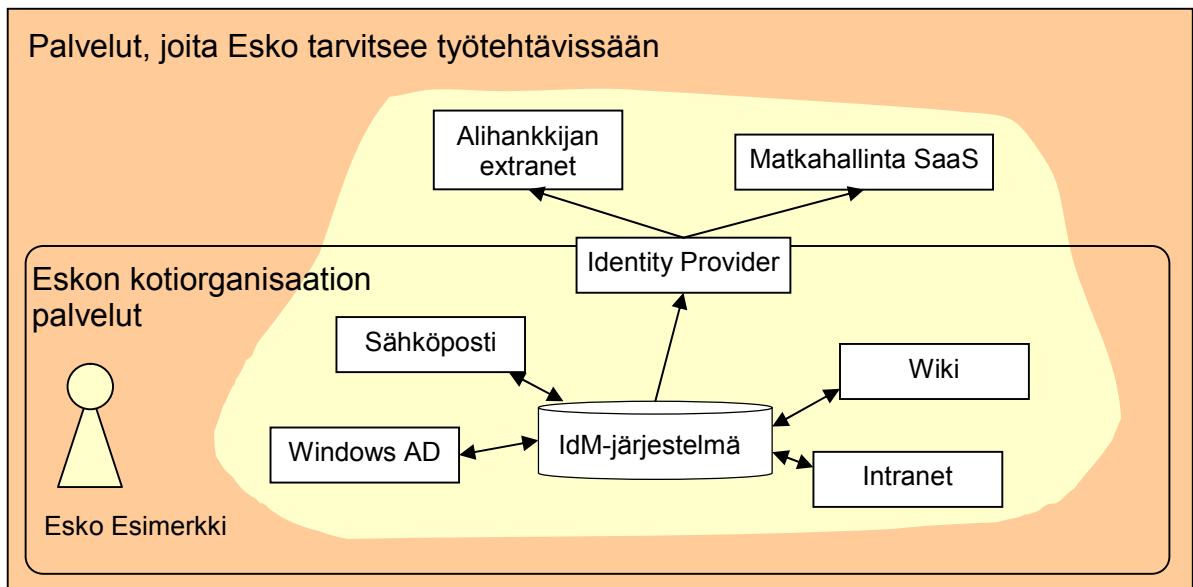


## 8. Federoitu identiteetinhallinta

Edellisessä luvussa tarkasteltiin tilannetta, jossa käyttäjän identiteettiä ja identiteettiin nojaavia tietojärjestelmiä hallinnoi yksi ja sama organisaatio. Suurimmat identiteetin- ja pääsynhallinnan tarpeet ovat toki usein käyttäjän omassa organisaatiossa; esimerkiksi organisaation työntekijällä on laajimmat käyttövaltuudet nimenomaan organisaation omissa sisäisissä tietojärjestelmissä.

Verkottuneessa ja verkostoituneessa yhteiskunnassa on kuitenkin yhä enemmän käyttötilanteita, joissa käyttäjän identiteettiä hallinnoi eri organisaatio kuin palvelua, joka nojaa käyttäjän identiteettiin. Tyypillinen tilanne on, että organisaation työntekijä joutuu osana työtehtäviään kirjautumaan organisaatiolle palveluja toimittavan toisen organisaation järjestelmiin, esimerkiksi extranet- tai SaaS-palveluun.

Tässä luvussa kutsutaan **kotiorganisaatioksi** sitä organisaatiota, johon käyttäjällä on sidos (esimerkiksi työntekijän työnantaja tai opiskelijan oppilaitos). Sidoksen perusteella käyttäjällä on käyttövaltuuksia toisen organisaation ylläpitämään tietojärjestelmään.



**Kuva 20. Federoitu identiteetinhallinta. Keltainen alue kuvastaa yhden identiteetin kattavuutta.**

Voidaan toki käyttää järjestelyä, jossa käyttäjän kotiorganisaatiossa on pääkäyttäjä, joka käsin hallinnoi organisaation työntekijöiden käyttäjätunnuksia ja -valtuuksia kotiorganisaation ulkopuolisessa tietojärjestelmässä. Tässä luvussa tarkastellaan kuitenkin järjestelyä, jossa organisaation ulkopuolisten tietojärjestelmien identiteetin- ja pääsynhallinta ripustetaan teknisellä kytkennällä (Kuva 20) organisaation sisäiseen identiteetinhallintajärjestelmään, joka esiteltiin edellisessä luvussa. Tätä kutsutaan **federoiduksi identiteetinhallinnaksi** (federated identity management). Se ei korvaa tai vähennä organisaation sisäisen identiteetinhallinnan merkitystä, vaan päin vastoin saattaa myös organisaation ulkopuoliset palvelut sen piiriin.

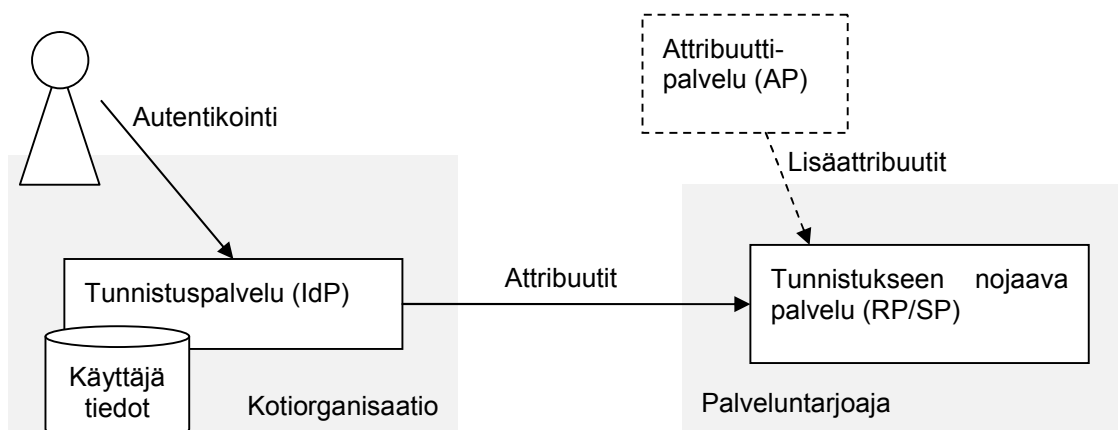
Tässä luvussa käydään ensin läpi federoidun identiteetinhallinnan peruskäsitteitä, hyötyjä ja tekniikoita. Organisaatiokeskeisen identiteetinhallinnan vastakohtana esitellään lopuksi käyttäjäkeskeinen federoitu identiteetinhallinta, jossa käyttäjä ei käytä palveluita kotiorganisaationsa edustajana.

## 8.1. Peruskäsitteet

Federoidun identiteetinhallinnan peruskomponentit ovat

- Tunnistuspalvelu (Identity Provider, IdP), joka on palvelin, jolla on käytettävissään ajantasainen tieto käyttäjän identiteetistä (attribuuteista) ja joka kirjautumishetkellä suorittaa käyttäjän tunnistamisen eli autentikoinnin. Tunnistuspalvelun omistavaa organisaatiota kutsutaan käyttäjän kotiorganisaatioksi.
- Tunnistukseen nojaava palvelu (Relying Party, RP tai Service Provider, SP), joka on palvelin, joka nojaa pääsynvalvonnassaan tunnistuspalvelun suorittamaan käyttäjätunnistukseen ja tunnistuspalvelusta saataviin käyttäjän attribuutteihin. Tunnistukseen nojaava palvelu on se ”varsinainen” sovellus, joka tarvitsee käyttäjän tunnistusta.

Oheinen kuva (Kuva 21) selventää tilannetta. Käyttäjän tunnistuksen esimerkiksi käyttäjätunnuksella ja salasanalla suorittaa tunnistuspalvelu, joka tunnistuksen suoritettuaan ojentaa käyttäjän tarpeelliset attribuutit standardin protokollan avulla tunnistukseen nojaavalle palvelulle, joka tekee pääsynvalvontapäätöksen<sup>12</sup>. Ero organisaation sisäiseen pääsynhallintaratkaisuun on lähinnä se, että tunnistukseen nojaava palvelu ei ole käyttäjän kotiorganisaation (esimerkiksi työnantajan) hallinnassa. Tunnistuspalvelu puolestaan tyypillisesti nojaa käyttäjän kotiorganisaation identiteetinhallintajärjestelmään, jota käsiteltiin edellä luvussa 7.



**Kuva 21. Federoidun identiteetinhallinnan perustoimijat ovat tunnistuspalvelu (IdP), jonka omistaa käyttäjän kotiorganisaatio ja tunnistukseen nojaava palvelu (RP/SP), jonka omistaa palveluntarjoaja.**

Lähtökohta on, että käyttäjän perustiedot saadaan aina kirjautumishetkellä tunnistuspalvelusta, jossa kotiorganisaatio huolehtii niiden ajantasaisuudesta. Tunnistukseen nojaava palvelu voi toki säilöä paikallisesti käyttäjään liittyviä lisäattribuuteja, kuten hänen profilinsa ja asetuksensa palvelussa. Jos tarkoituksenmukaista on, että käyttäjään liittyviä lisäattribuutteja ylläpidetään keskitetysti kotiorganisaation ulkopuolella, voidaan tunnistuspalvelun ja tunnistukseen nojaavan palvelun lisäksi ajatella kolmanneksi palvelutyypiksi attribuuttipalvelu (Attribute Provider, AP), joka ylläpitää ja

<sup>12</sup> Federoidussa identiteetinhallinnassa transaktio (autentikointi, attribuuttien luovutus ja pääsynvalvontapäätös) tapahtuu siis kirjautumishetkellä. Luvun 3.1 termien valossa pitäisikin oikeastaan puhua federoidusta pääsynhallinnasta, mutta federoitu identiteetinhallinta on terminä vakiintuneempi.

antaa tunnistuspalvelun tunnistamille käyttäjille kuuluvia lisäattribuutteja tunnistukseen nojaaville palveluille.

Organisaatiokeskeisessä federoidussa identiteetinhallinnassa leimallista on käyttäjän vahva sidos hänen kotiorganisaatioonsa, joka ylläpitää tunnistuspalvelua. Käyttäjä voi esimerkiksi olla kotiorganisaation työntekijä tai muu sisäinen käyttäjä, ja kotiorganisaatiolla on keskeinen rooli käyttäjän tunnistuksen ja attribuuttien luotettavuuden takaajana.

## 8.2. Federoidun identiteetinhallinnan hyötyjä

Federoidun identiteetinhallinnan hyödyt noudattavat pitkälti luvussa 2 esiteltyjä identiteetin- ja pääsynhallinnan kehittämisen hyötyjä.

Tietoturvaa kohentavia hyötyjä ovat

- Käyttäjän **käyttäjätunnuksen sulkeminen kotiorganisaatiossa** sulkee käyttäjän pääsyn tunnistukseen nojaaviin palveluihin. Riittää siis, että kotiorganisaatio muistaa sulkea käyttäjätunnuksen tunnistuspalvelussa, eikä käyttäjätunnusta tarvitse erikseen muistaa sulkea jokaisessa tunnistukseen nojaavassa palvelussa.
- Tunnistuspalvelu voidaan **sijoittaa kotiorganisaation sisäverkkoon**, jossa se ei ole lainkaan näkyvissä sisäverkon ulkopuolelle. Näin hyökkäyksille altistuva hyökkäyspinta vähenee. Hyökkääjän pitää ensin onnistua tunkeutumaan sisäverkkoon, ennen kuin hän voi yrittää kirjautumista tunnistukseen nojaavaan palveluun.
- Käyttäjän **käyttäjätunnus ja salasana eivät koskaan käy** tunnistukseen nojaavassa palvelussa, koska käyttäjätunnus ja salasana annetaan aina ja vain tunnistuspalvelulle. Niinpä nojaavaan palveluun murtautumisesta ei voi seurata käyttäjätunnusten ja salasanojen vuotaminen Internetiin, mikä loisi hyökkääjille edellytykset kokeilla samojen käyttäjätunnusten ja salasanojen sopimista muihin palveluihin.
- Koska käyttäjällä on vain yksi käyttäjätunnus ja salasana, jolla hän kirjautuu tunnistuspalveluun, voidaan **salasanaan kohdistaa tiukempia laatuvaatimuksia**. Salasana voi esimerkiksi olla pidempi ja sille voidaan pakottaa tiheämpi vaihtumisväli. Siitä huolimatta voidaan kohtuudella olettaa, että käyttäjän ei tarvitse kirjoittaa salasanaa ylös.
- Jos salasanatunnistus halutaan korvata vahvemmallalla tunnistuksella, kotiorganisaatio voi **ottaa vahvan tunnistuksen käyttöön keskitetysti** tunnistuspalvelussa. Näin vahva tunnistus saadaan kaikkien nojaavien palveluiden ulottuville kertaheitolla ilman, että nojaaviin palveluihin tarvitsee tehdä muutoksia.
- Jos käyttäjän kirjautuminen palveluihin tapahtuu aina keskitetyn tunnistuspalvelun kautta, **jäljitettävyyys- ja raportointi helpottuu**. Jos on esimerkiksi syytä epäillä, että käyttäjätili on joutunut tunkeutujan haltuun, voidaan tunnistuspalvelun lokeista selvittää, missä kaikissa palveluissa varastettua identiteettiä on käytetty.

Tehokkuutta kohentavia hyötyjä ovat

- Käyttäjän **ei tarvitse muistaa montaa käyttäjätunnus/salasana-paria**, mikä vähentää unohtuneiden salasanojen muisteluun ja selvittelyyn kuluva aikaa.
- Vastaavasti unohtuneiden **salasanojen nollaamiseen IT-tuessa** kuluva aika vähenee.

- Saman käyttäjän **päällekkäisten käyttäjätietojen ylläpitäminen vähenee**, kun tunnistukseen nojaava palvelu saa ajantasaiset käyttäjätiedot tunnistuspalvelusta.

Lisäksi federoitu käyttäjätunnistus saattaa osaltaan luoda edellytyksiä organisaation toimintojen järjestämiseen uudella tavalla. Palveluja on esimerkiksi helpompi ulkoistaa (Software as a Service, pilvipalvelut), kun palvelun ulkoistaminen ei edellytä uusien käyttäjätunnus/salasana-parien antamista käyttäjille.

### 8.3. Luottamus ja luottamusmallit

Ehkä suurimpia federoidun identiteetinhallinnan haasteita on organisaatioiden välinen luottamus. Luottamuksella tarkoitetaan sitä **laajuutta, jossa toimija on halukas olemaan tiettyssä asiassa riippuvainen toisesta toimijasta ja kokee olonsa suhteellisen turvalliseksi, vaikka olemassa on myös mahdollisuus negatiivisesta seurauksesta**. Toisin sanoen:

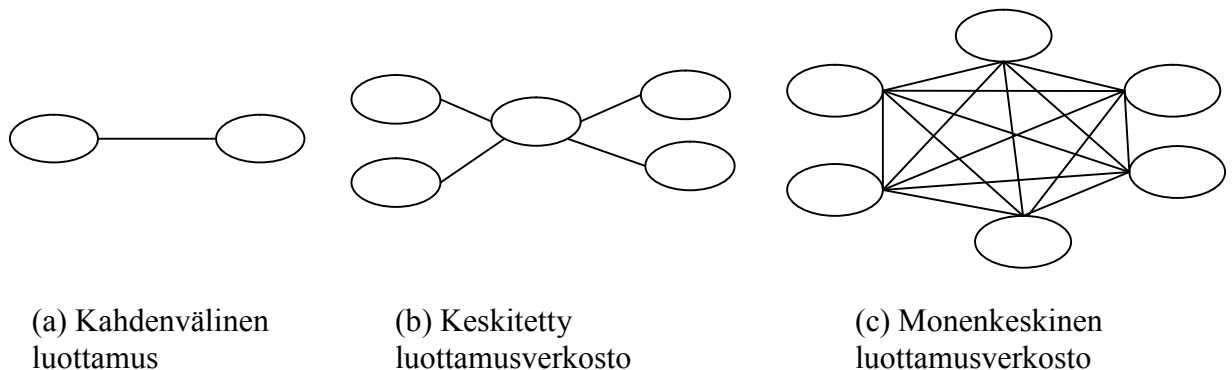
- On olemassa mahdollisuus negatiivista seuraamuksista (eli riski),
- Luottava taho on riippuvainen luottamuksen kohteesta,
- Luottava taho kokee riippuvuussuhteesta huolimatta tilansa suhteellisen turvalliseksi,
- Luottava taho ei pysty kontrolloimaan luottamuksen kohdetta, ja
- Luottamus liittyy tiettyyn asiaan (esimerkiksi identiteetinhallintaan muttei lentokoneen ohjaamiseen).

Koska tunnistuspalvelua ja tunnistukseen nojaava palvelua ylläpitävät eri organisaatiot, nousee keskeiseen asemaan kysymys organisaatioiden välisestä luottamuksesta.

- Tunnistukseen nojaavan palvelun tulee luottaa, että tunnistuspalvelu on **tunnistanut käyttäjän riittävän luotettavalla tavalla**. Riittävä luotettavuus riippuu nojaavasta palvelusta – mitä sensitiivisempi palvelu on, sitä luotettavammin käyttäjä tulee tunnistaa. Tunnistuksen luotettavuutta ja sitä kuvaavia viitekehyksiä käsiteltiin luvussa 4.3. Voidaan ajatella, että yksi tunnistuspalvelun nojaavalle palvelulle ojentamista attribuuteista on tieto suoritettujen käyttäjätunnistuksen vahvuudesta.
- Tunnistukseen nojaavan palvelun tulee luottaa, että tunnistuspalvelun sille ojentavat **attribuutit ovat oikein ja ajan tasalla**. Nojaavan palvelun tekemä pääsynvalvontapäätös saattaa nojata käyttäjän attribuutteihin. Nojaavan palvelun täytyy lisäksi luottaa siihen, että käyttäjän kotiorganisaatio on muistanut sulkea hänen käyttäjätunnuksensa, jos käyttäjä on poistunut kotiorganisaation palveluksesta tai käyttäjätunnuksen peruste kotiorganisaatiossa on lakannut muusta syystä.
- Tunnistuspalvelun tulee luottaa siihen, että tunnistukseen nojaava palvelu **ei loukkaa käyttäjän yksityisyyttä** käsitellessään tunnistuspalvelun sille ojentamia attribuutteja. Koska käyttäjän attribuutit täyttävät yleensä henkilötiedon määritelmän, voidaan myös tunnistuspalvelua pitää osaksi vastuullisena mahdollisesta tietomurrosta tai muusta tietosuojaongelmasta tunnistukseen nojaavassa palvelussa. Henkilötietolakia käsitellään lisää luvussa 9.

Osapuolet joutuvat hallitsemaan riskiä siitä, että vastapuoli ei ole siihen kohdistetun luottamuksen arvoinen. Keskeinen tapa hallita riskiä on sopia osapuolten kesken niistä oikeuksista ja velvollisuuksista, joita federoituun identiteetinhallintaan liittyy. Sopimus sisältää paitsi teknisiä asioita (esimerkiksi käytettävät protokollat, varmenteet ja

attribuuttien skeema), myös toimintakäytäntöihin liittyviä asioita (esimerkiksi tunnistuksen luotettavuudelle ja attribuuttien ajantasaisuudelle ja palvelun saatavuudelle asetettavat vaatimukset). Oheinen kuva (Kuva 22) havainnollistaa erilaisia malleja rakentaa osapuolten väliset luottosuhteet.



**Kuva 22. Luottamusmallit**

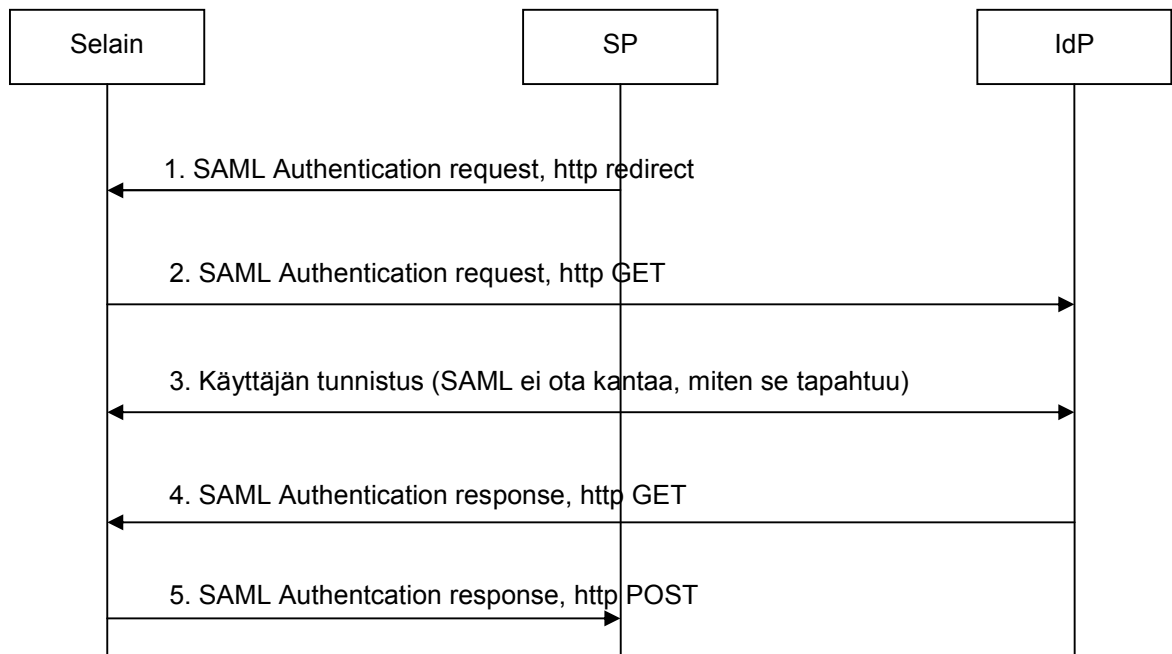
Kuvan (a)-kohdassa kaikki luottamussuhteet perustuvat suoriin kahdenvälisiin järjestelyihin. Palveluntarjoaja ja kotiorganisaatio sopivat aina kahdenvälisesti federoidun tunnistuksen käyttöön liittyvistä vastuista ja järjestelyistä. Tämä vaihtoehto soveltuu käytettäväksi esimerkiksi silloin, kun federoitu tunnistus liittyy kotiorganisaation palveluntarjoajalta ostamaan palveluun (esim. SaaS-palvelu), josta laaditaan joka tapauksessa kahdenvälinen sopimus. Tällöin sopimus voi kattaa myös federoituun tunnistukseen liittyvät asiat.

Jos kotiorganisaatioita ja palveluntarjoajia on paljon, saattaa luottamusverkostomainen toimintatapa helpottaa toimintaa. Luottamusverkostossa useita kotiorganisaatioita ja palveluntarjoajia on yhdessä ottanut käyttöön federoituun identiteetinhallintaan perustuvan käyttäjätunnistuksen ja sopinut siihen liittyvistä vastuista ja järjestelyistä. Luottamusverkosto saattaa olla sopimuksellisessa ja/tai teknisessä mielessä keskitetty, eli rakentua luottamusverkostoa operoivan keskusorganisaation ympärille (kuvan (b)-kohta). Luottamusverkosto voi olla myös täysin hajautettu (kuvan (c)-kohta).

#### **8.4. Teknologioista**

Federoidun identiteetinhallinnan tunnetuin teknologia WWW-ympäristössä on SAML (Security Assertion Markup Language), jonka versiosta 2.0 on saatavilla lukuisia kaupallisia ja avoimen lähdekoodin toteutuksia. SAML on XML-pohjainen kieli (määrittelee oikein muodostettujen SAML-sanomien syntaksin ja semantiikan) ja protokolla (määrittelee, kuinka pyyntöihin vastataan vastauksilla) tietoturvallisuutta koskevien väittämien (assertion, claim) välittämiseen.

SAML-sanomien kuljettaminen (sidos, engl. binding) tapahtuu yleensä joko SOAP-protokollan avulla tai WWW-selaimen välityksellä, jolloin SAML-sanoma lastataan selaimen tekemän http POST –pyynnön sisältöön tai http redirect –pyynnön URL-osoitteen loppuun. SAML-sanomien eheys voidaan taata XML-allekirjoituksella ja luottamuksellisuus XML-salauksella.



**Kuva 23. SAML-protokollan yleisin käyttötilanne on WWW-kirjautuminen.**

Oheinen viestisekvenssikaavio (Kuva 23) kuvaa SAML-teknologian tavallisimman käyttötilanteen, joka on SAML Authentication Request protocol, joka nojaa selaimen välittämään http POST ja redirect -sidokseen. Huomaa, kuinka protokolla käyttää loppukäyttäjän selainta SAML-sanomien kuljettamiseen IdP- ja SP-palvelimen välillä. SAML-määrittely kutsuu tunnistukseen nojaavaa palvelinta Service Provideriksi (SP).

1. Käyttäjä on painanut ”kirjaudu sisään” –nappulaa www-sivulla, ja SP tulostaa käyttäjän selaimen http-vastauksen, joka komentaa selaimen uudelleenohjautumaan (http redirect) IdP-palvelimelle. Uudelleenohjauksen URL-loppuosa sisältää SAML Authentication Request –sanoman.
2. Selain uudelleenohjautuu IdP-palvelimelle, jolloin IdP-palvelin vastaanottaa selainpyynnön (http GET) mukana tulevan SAML Authentication request –sanoman.
3. Tämän jälkeen IdP suorittaa käyttäjän tunnistuksen tavalla, jota SAML ei määrittele. Käyttäjä voi esimerkiksi tunnistautua IdP-palvelimelle salasanalla, varmenteella, tai IdP-palvelin voi nojata vaikkapa Windows-toimialuekirjautumiseen. Jos IdP-palvelin on jo tunnistanut käyttäjän, ei loppukäyttäjää tarvitse häiritä lainkaan, vaan hän pääsee nauttimaan kertakirjautumisesta (usein käyttötapauksista kutsutaankin tämän vuoksi SAML Web Single sign-on –käyttötapaukseksi).
4. IdP-palvelin muodostaa SAML Authentication response –sanoman ja sisällyttää siihen käyttäjän yksilöivän tunnisteen ja tarpeellisen määrän hänen attribuuttejaan, sekä muun muassa tiedon käyttäjätunnistuksen suorittajasta, suoritustavasta ja -hetkestä. Vastaus allekirjoitetaan digitaalisesti, tarvittaessa salataan ja lähetetään lopuksi selaimen.
5. Selain välittää saamansa sivun SP:lle http POST –pyynnöllä. SP vastaanottaa pyynnön, varmistaa SAML-sanoman aitouden ja eheyden ja poimii sanomasta käyttäjän attribuutit.

SAML on siis lähinnä pääsynvalvontaa tukeva protokolla, jota käytetään käyttäjän tunnistuksen ”federoimiseen” hänen kotiorganisaatiostaan tunnistukseen nojaavaan palveluun. Käyttäjän tunnistuksen, tunnistetusta käyttäjästä siirrettävien attribuuttien ja tunnistetusta käyttäjästä palveluun mahdollisesti aikaisemmin talletettujen tietojen (kuten käyttövaltuuksien) perusteella tunnistukseen nojaava palvelu tekee pääsynvalvontapäätöksensä.

On hyvä huomata, että SAML-teknologiaa ei ole tarkoitettu käyttäjän identiteettien ja käyttövaltuuksien provisiointiin ja deprovisiointiin kotiorganisaatiosta käsin palveluihin. SAML-teknologian avulla kotiorganisaatio ei voi esimerkiksi järjestää joka yö tapahtuvaa eräajoa, jossa palveluun perustetaan uusien käyttäjien käyttäjätunnukset ja käyttövaltuudet, ja organisaatiosta poistuneiden käyttäjien käyttövaltuudet suljetaan. Tämän toteuttamiseen soveltuvia teknologioita ovat esimerkiksi SPML (Simple Provisioning Language Markup) ja SCIM (Simple Cloud Identity Management). SAML-teknologia nojaa myös vahvasti http-protokollan ominaisuuksiin, mikä on ongelmallista muille kuin selainpalveluille, kuten matkapuhelinten natiivisovelluksille.

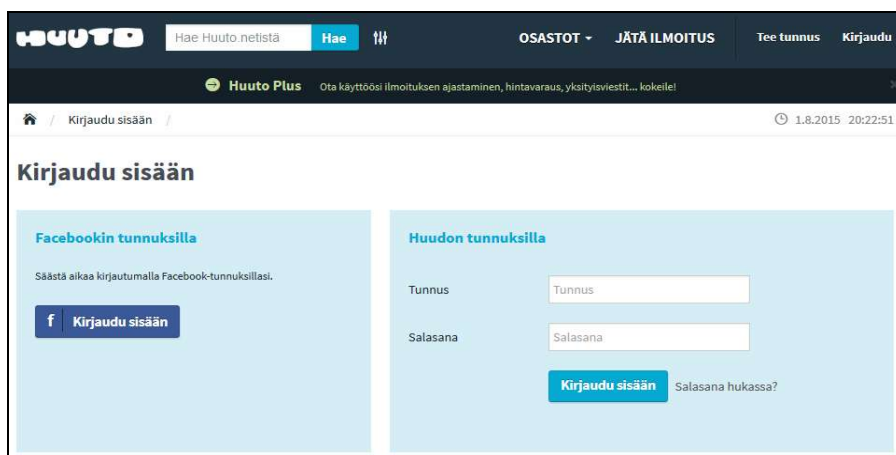
Lisätietoa:

[www.oasis-open.org/committees/security/](http://www.oasis-open.org/committees/security/)

## 8.5. Käyttäjäkeskeinen identiteetinhallinta

Edellä on käsitelty federoitua identiteetinhallintaa organisaatiokeskeisestä näkökulmasta. Käyttäjällä on vahva sidos kotiorganisaatioonsa, joka vastaa tunnistuspalvelusta ja sen suorittamasta käyttäjätunnistuksesta ja attribuuttien ajantasaisuudesta. Organisaatiokeskeinen identiteetinhallinta on luontevaa tilanteessa, jossa käyttäjä toimii tunnistukseen nojaavassa palvelussa kotiorganisaationsa jäsenenä ja edustajana. Tämä on tilanne esimerkiksi silloin, kun organisaation työntekijä kirjautuu ulkoistettuun palveluun (Software as a Service, pilvipalvelut) tai organisaatiolle palveluja toimittavan yrityksen extranet-palveluun.

Organisaatiokeskeisen federoidun identiteetinhallinnan vastakohta on käyttäjäkeskeinen (user centric) federoitu identiteetinhallinta, joka ei perustu käyttäjän ja kotiorganisaation vahvalle sidokselle. Sen sijaan käyttäjä tyypillisesti käyttää palvelua yksityishenkilönä ja vastaa itse omasta identiteetistään ja siihen tunnistuspalvelussa mahdollisesti liittyvistä attribuuteista.



The screenshot shows the login page of Huuto.net. At the top, there is a navigation bar with the Huuto logo, a search bar, and links for 'OSASTOT', 'JÄTÄ ILMOITUS', 'Tee tunnus', and 'Kirjaudu'. Below the navigation bar, there is a section titled 'Kirjaudu sisään' (Log in). On the left, there is a box for logging in with Facebook credentials, labeled 'Facebookin tunnuksilla'. On the right, there is a box for logging in with Huuto credentials, labeled 'Huudon tunnuksilla'. The Huuto login box contains fields for 'Tunnus' (Username) and 'Salasana' (Password), and a 'Kirjaudu sisään' button. There is also a link for 'Salasana hukassa?' (Forgot password?).

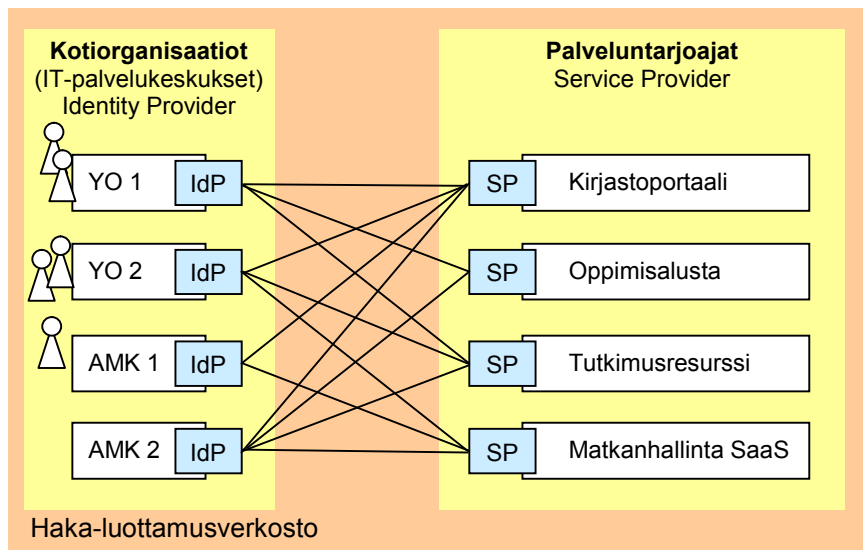
Kuva 24. Esimerkki verkkopalvelusta, joka on ottanut käyttäjäkeskeisen federoidun tunnistamisen (vasemmalla) palvelun sisäisen käyttäjätunnuksen/salasanan (oikealla) rinnalle. Kuva: Huuto.net.

Käyttäjakeskeisessä identiteetinhallinnassa kotiorganisaatio ei takaa käyttäjän identiteetin ja attribuuttien luotettavuutta – käyttäjä voi siis kenenkään estämättä esiintyä vaikkapa Aku Ankkana. Tätä ei kuitenkaan pidetä ongelmallisena, vaan se on käyttäjakeskeisen identiteetinhallinnan ominaisuus. Käyttäjakeskeisen identiteetinhallinnan tarkoitus ei ole tarjota vahvan ensitunnistukseen perustuvaa identiteettiä, vaan poistaa käyttäjän tarve rekisteröityä ja perustaa käyttäjätili erikseen jokaiseen Internetissä olevaan www-palveluun. Jos www-palvelua ei haittaa, että siihen rekisteröityy suoraan Aku Ankka – pseudonyymiä käyttävä henkilö, on palvelulle yhdentekevää, jos siihen suorittaa federoidun kirjautumisen Aku Ankka –niminen käyttäjä.

Käyttäjakeskeinen federoitu identiteetinhallinta yhdistetään usein OpenID-nimiseen tekniikkaan, jonka kolmas sukupolvi on OpenID Connect. Periaatteessa kuka vain voi asentaa OpenID Connect -tunnistuspalvelun ja alkaa tarjota käyttäjätunnistusta tunnistukseen nojaaville tahoille. Käytännössä tunnistuspalvelun roolin ovat omaksuneet kuitenkin Internetin suuret ylikansalliset toimijat kuten Google tai Facebook, joissa sadoilla miljoonilla käyttäjillä on käyttäjätilit valmiina. Tällöin tunnistukseen nojaava palvelu laittaa kirjautumissivulleen kyseisen tunnistuspalvelun kirjautumisnapin (Kuva 24).

## 8.6. Esimerkkejä federoidun identiteetinhallinnan palveluista

Haka on Suomen korkeakoulujen ja tutkimuslaitosten yhteinen käyttäjätunnistusjärjestelmä, joka nojaa SAML 2.0 –teknologiaan. Opiskelija, opettaja tai tutkija käyttää kotikorkeakoulunsa käyttäjätunnusta ja salasanaa kirjautuessaan Haka-tunnistukseen nojaaviin palveluihin, kuten oppimisalustoihin, korkeakoulukirjastojen sähköisiin palveluihin, tutkimusresursseihin ja talous- ja henkilöstöhallinnon palveluihin. Samalla kotikorkeakoulun tunnistuspalvelu ojentaa tunnistukseen nojaavalle palvelulle tämän käyttäjästä tarvitsemat attribuutit, kuten nimen, yhteystiedot ja hänen roolinsa kotikorkeakoulussaan.



**Kuva 25. Haka-käyttäjätunnistusjärjestelmä perustuu korkeakoulujen muodostamaan luottamusverkostoon.**

Haka-luottamusverkostoa operoi Tieteen tietotekniikan keskus CSC, joka solmii sopimuksen tunnistuspalvelun käytöstä luottamusverkostoon liittyvien organisaatioiden



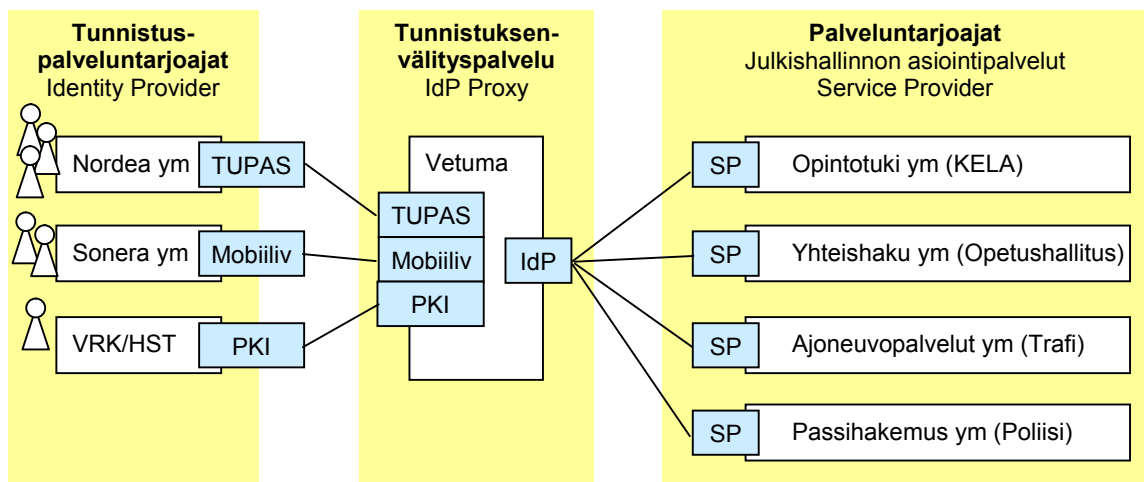
kanssa. Luottamusmalliltaan Haka on siis hallinnolliselta rakenteeltaan keskitetty luottamusverkosto (Kuva 22 b). Tunnistuspalvelut ja tunnistukseen nojaavat palvelut vaihtavat SAML-viestejä kuitenkin suoraan toistensa kanssa, eli tekninen rakenne on hajautettu. Elokuussa 2015 Hakassa oli 44 tunnistuspalvelua ja 219 tunnistukseen nojaavaa palvelua.

Lisätietoa: [www.csc.fi/haka](http://www.csc.fi/haka)

Suomessa yksityishenkilöiden vahva sähköinen tunnistaminen nojaa pitkälti yksityisen sektorin tarjoamiin maksullisiin palveluihin, erityisesti pankkien **TUPAS**-tunnistuspalveluun. TUPAS on Finanssialan keskusliiton laatima ja julkaisema selainpohjainen protokollamäärittäjä, jonka mukainen tunnistuspalvelu (Identity Provider) on saatavilla kymmenestä Suomessa toimivasta pankista tai pankkiryhmästä. Tunnistukseen nojaava taho solmii pankin kanssa kahdensivuisen sopimuksen tunnistuspalvelun käytöstä ja suorittaa pankille muutaman kymmenen sentin suuruisen maksun jokaisesta tunnistustapahtumasta.

Lisätietoa:  
[www.fkl.fi/teemasivut/sahkoinen\\_asiointi/tupas/](http://www.fkl.fi/teemasivut/sahkoinen_asiointi/tupas/)

Jotta jokaisen julkishallinnon asiointipalvelun ei tarvitsisi rakentaa teknistä integraatiota erikseen jokaiseen tunnistuspalveluntarjoajaan, on valtionhallinto ottanut käyttöön **Vetuma**-nimisen keskitetyn tunnistuspalvelun, joka toimii päälystakkina yksityissektorin tunnistuspalveluille. Vetuma on julkishallinnon yhteinen tunnistuspalvelu, jonka tarjoamaa rajapintaa vasten julkishallinnon sähköiset asiointipalvelut voivat suorittaa kansalaisen vahvan tunnistamisen.



**Kuva 26.** Vetuma on julkishallinnon yhteinen tunnistuksenvälityspalvelu, jonka kautta julkishallinnon sähköiset asiointipalvelut voivat tunnustaa kansalaisen yhtä teknistä rajapintaa vasten verkkopankkitunnuksilla, mobiilivarmenteella tai sähköisellä henkilökortilla.

Teknisesti Vetuma on tunnistuksenvälityspalvelu (Kuva 26), joka tarjoaa asiointipalveluille SAML-rajapinnan tai TUPAS-protokollaa muistuttavan kutsurajapinnan, johon asiointipalvelu ohjaa tunnistettavan käyttäjän. Vetuma ohjaa käyttäjän tunnistettavaksi hänen valitsemaansa tunnistuspalveluun, ja palauttaa asiointipalvelulle käyttäjän autentikoidun identiteetin (henkilötunnuksen). Tällä hetkellä Vetuma tukee tunnistautumista pankkien verkkopankkitunnuksilla (TUPAS), mobiilivarmenteella (teleoperaattorien tukema ETSI 102 204 -protokolla, katso luku 4.5) tai sähköisellä

henkilökortilla olevalla Väestörekisterikeskuksen kansalaisvarmenteella (PKI ja TLS-asiakkaan tunnistus, katso luku 4.5). Kesäkuussa 2015 98% Vetuma-tunnistuksista suoritettiin verkkopankkitunnuksilla.

Lisätietoa: <a href="http://www.suomi.fi/vetuma">www.suomi.fi/vetuma</a>
--

## 8.7. Pohdittavaa

- Monet organisaatiot ovat huomanneet, että SAML-teknologiaa voidaan käyttää myös organisaation sisäisten www-palveluiden kertakirjautumistekniikkana. Mitä etua tästä saadaan? Entä mitkä organisaatorajat ylittävän kirjautumisen haasteet muuttuvat tällöin helpommiksi?
- Luvussa 8.6 esiteltiin Haka-käyttäjätunnistusjärjestelmän hajautettu ja Vetuma-palvelun yhteen keskitettyyn palveluun nojaava tekninen arkkitehtuuri. Vertaile näitä kahta periaatetta saatavuuden, suorituskyvyn, tietoturvan ja tietosuojan kannalta. Mitä etua Vetuman arkkitehtuuri tuo, jos käytössä on tekniikaltaan erilaisia tunnistuspalveluntarjoajia (kuten Tupas ja PKI)? Kumpi on helpompi malli ongelmien selvittelyssä?
- Organisaatiokeskeisen identiteetinhallinnan kulmakivenä pidettiin käyttäjän vahvaa sidosta hänen kotiorganisaatioonsa, joka käyttäjäkeskeisessä identiteetinhallinnassa puuttuu. Toisaalta kerrottiin, että käyttäjäkeskeinen identiteetinhallintakin on käytännössä luiskahtanut siihen, että käyttäjä käyttää tunnistuspalvelunaan esimerkiksi Googlea, jonka asiakas hän on. Onko käyttäjäkeskeinen identiteetinhallinta tosiasiassa muuttunut organisaatiokeskeiseksi identiteetinhallinnaksi?

## 9. Tietosuoja ja henkilötietolaki

Lopuksi käsitellään henkilötietolakia identiteetinhallinnan näkökulmasta. Tarkastelun tarkoitus on antaa lukijalle yleiskuva niistä vaatimuksista, joita identiteetin- ja pääsynhallinnalle seuraa henkilötietolaista, joka on henkilötietojen käsittelyä säätelevä yleislaki. Tässä luvussa ei tarkastella soveltamisalaltaan rajattuja erityislakeja, kuten työelämän tietosuojalakia tai tietoyhteiskuntakaarta.

Tietojärjestelmien käyttäjätietokannassa olevat identiteetit voidaan tyypillisesti tunnistaa luonnollista henkilöä koskeviksi merkinnöiksi, jolloin henkilötiedon määritelmä täyttyy ja käyttäjätietokantaa pidetään henkilörekisterinä. Tällöin käyttäjää kutsutaan rekisteröidyksi, käyttäjätietokannan omistavaa organisaatiota rekisterinpitäjäksi, ja kaikkia käyttäjätietoihin kohdistuvia toimenpiteitä henkilötietojen käsittelyksi.

### 9.1. OECD:n tietosuojaperiaatteet ja tietosuojadirektiivi

Eurooppalainen tietosuojalainsäädäntö perustuu OECD:n 1980-luvulla antamaan tietosuojaperiaatteita koskevaan suositukseen:

1. **Informointivelvoite** – rekisteröityä tulisi informoida häntä koskevien henkilötietojen keräämisestä ja käsittelystä.
2. **Käyttötarkoitussidonnaisuus** – henkilötietojen käsittelyn tarkoitus tulisi suunnitella etukäteen, eikä henkilötietoja saisi käsitellä muihin tarkoituksiin.
3. **Tarpeellisuusvaatimus** – käsiteltävien henkilötietojen tulisi olla henkilörekisterin käyttötarkoituksen kannalta tarpeellisia, ja henkilötietojen ajantasaisuudesta tulisi huolehtia.
4. **Rekisteröidyn suostumus** – henkilötietoja ei tulisi käsitellä ilman rekisteröidyn suostumusta, ellei laissa säädetä muuta. Suostumuksen yksi piirre on, että rekisteröity voi koska vain peruuttaa sen.
5. **Suojaamisvelvoite** – rekisterinpitäjän tulisi suojata kerätyt henkilötiedot väärinkäytön varalta.
6. **Tarkistus- ja korjausoikeus** – rekisteröidyllä tulisi olla oikeus tarkistaa, mitä henkilötietoja rekisterinpitäjällä on hänestä, ja tarpeen mukaan oikaista virheelliset henkilötiedot.
7. **Tilivelvollisuus** – rekisterinpitäjä tulisi pitää tilivelvollisena näiden periaatteiden noudattamisesta, vaikka tämä olisikin ulkoistanut henkilötietojen käsittelyn toiselle organisaatiolle.

OECD:n suositukset ovat olleet perustana EU:n tietosuojadirektiiville (95/46/EY), joka on implementoitu Suomen lainsäädäntöön henkilötietolailla. Muilla EU- ja ETA-mailla on pääpiirteissään samansisältöiset henkilötietolait. Tällä hetkellä EU valmistelee tietosuojadirektiivin korvaavaa yleistä tietosuoja-asetusta.

Lisätietoa: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data Henkilötietolaki 22.4.1999/523
---

## 9.2. Suojaamisvelvoitteesta

Suomen lainsäädännöstä ei löydy yleiskattavaa tietoturvalakia, joka velvoittaisi tietojärjestelmän ylläpitäjää huolehtimaan järjestelmänsä tietoturvallisuudesta asianmukaisella tavalla. Jos tietojärjestelmä kuitenkin sisältää henkilötietoja, jotka muodostavat henkilörekisterin, seuraa mainittu velvoite henkilötietolaista. Henkilötietolain mukaan rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsylvä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä.

Suojaamisvelvoitteeseen sisältyy kuitenkin tietoturvallisuudessa yleensä käytetty periaate riskien ja suojaamisesta aiheutuvien kustannusten tasapainottamisesta. Rekisterinpitäjän on nimittäin suojauksia toteuttaessaan otettava huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta. Voidaan siis ajatella, että mitä suuremmat rekisteröidyn yksityisyyteen liittyvät riskit realisoituisivat henkilörekisterin suojausten pettäessä, sitä ankarampi suojaamisvelvoite rekisterinpitäjällä on.

Mitkä henkilötiedot sitten ovat rekisteröidyn yksityisyyden suojan kannalta erityisen sensitiivisiä? Henkilötietolaki vastaa tähän kysymykseen määrittelemällä arkaluontoisiksi henkilötiedoiksi merkinnät, jotka koskevat rekisteröidyn

- rotua tai etnistä alkuperää,
- yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista,
- rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta,
- terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia,
- henkilön seksuaalista suuntautumista tai käyttäytymistä taikka
- henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia.

Arkaluontoisia henkilötietoja ei saa käsitellä kuin laissa olevien poikkeuksin. Myös henkilötunnuksen käsittelystä on henkilötietolaissa omat erityissäännöksensä.

## 9.3. Henkilörekisteriseloste

Informointivelvoitteen toteutumisen varmistamiseksi henkilötietolaki velvoittaa rekisterinpitäjän laatimaan henkilörekisteriselosteen, joka on kaikkien saatavilla. Henkilörekisteriselosteesta ilmenee

- rekisterinpitäjän ja tämän yhteyshenkilön nimi ja yhteystiedot,
- henkilötietojen käsittelyn tarkoitus,
- mitä tietoja rekisteröidyistä henkilörekisteriin kerätään,
- mihin henkilötietoja luovutetaan säännönmukaisesti ja luovutetaanko niitä EU:n tai ETA:n ulkopuolelle,
- mitkä ovat rekisterin suojauksen periaatteet.

Lisäksi rekisterinpitäjän tulee kertoa, kuinka rekisteröity voi käyttää oikeuttaan tarkistaa ja korjata henkilörekisterissä olevat itseään koskevat merkinnät.

Lisätietoa: Tietosuojavaltuutetun toimisto  
[www.tietosuoja.fi](http://www.tietosuoja.fi)

#### 9.4. Loogisen rekisterin käsite

Organisaatiossa saattaa olla valtava määrä tietojärjestelmiä, jotka ovat henkilörekistereitä. Onhan niin, että jokainen tietojärjestelmä, joka tunnistaa käyttäjänsä, mitä ilmeisimmin käsittelee henkilötietoja. Tuleeko siis kaikista näistä henkilörekistereistä laatia tietosuojaseloste?

Henkilötietolaki määrittelee henkilörekisterin **käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä** muodostuvaksi henkilötietoja sisältäväksi tietojoukoksi. Tämä niin sanottu loogisen rekisterin käsite mahdollistaa siis käyttötarkoitukseltaan yhteenkuuluvien henkilörekistereiden niputtamisen yhdeksi loogiseksi kokonaisuudeksi. Esimerkiksi tietojärjestelmät, joissa työntekijöillä on käyttäjätunnuksia, ajatellaan organisaation henkilökuntarekisterin loogiseksi alirekisteriksi, eikä niistä tarvitse laatia erillistä rekisteriselostetta.

On kuitenkin tilanteita, joissa kaikkia organisaation rekistereitä ei voida ajatella henkilökuntarekisterin tai asiakasrekisterin loogiseksi alirekisteriksi, vaan erillisiksi rekistereiksi, joilla on eri käyttötarkoitus. Tyypillinen tilanne syntyy lokitiedoista, jotka sisältävät usein sensitiivisiäkin henkilötietoja. Kun asiakassuhde ja siten peruste käsitellä asiakkaan henkilötietoja päättyy, poistetaan asiakas asiakasrekisteristä ja sen loogisista alirekistereistä, kuten identiteetinhallintajärjestelmästä<sup>13</sup>. Yleensä kuitenkin henkilön toiminnasta lokiin jääneitä merkintöjä ei poisteta, koska organisaation lokitiedostot muodostavat asiakasrekisteristä erillisen, oman itsenäisen kokonaisuutensa, jolla on oma käyttötarkoituksensa, säilytysaikansa jne. Siinä missä asiakasrekisterin käyttötarkoitus lienee asiakassuhteen hoitaminen ja organisaation palveluiden tarjoaminen asiakkaalle, lokijärjestelmän muodostaman henkilörekisterin käyttötarkoitus lienee esimerkiksi tietojärjestelmien vikatilanteiden ja väärinkäytösten selvitys tai kapasiteetin riittävyyden seuranta.

#### 9.5. Henkilötietojen luovutus kolmansiin maihin

Tietosuojadirektiivi ja henkilötietolaki lähtevät siitä, että henkilötiedot voivat liikkua vapaasti EU:n ja Euroopan talousalueen (ETA:an kuuluvat lisäksi Norja, Islanti ja Liechtenstein) sisällä, kunhan henkilötietojen käsittelyssä noudatetaan henkilötietolakia. Tietosuojadirektiivin melko yhtenäiset kansalliset toteutukset ja tulkinnat takaavat henkilötiedoille riittävän suojan riippumatta siitä, minkä EU- tai ETA-maan lainsäädännön piirissä rekisterinpitäjä toimii.

EU/ETA-maiden ulkopuolella lainsäädäntö ei kuitenkaan välttämättä takaa henkilötiedoille yhtä korkeaa suojaa. EU-lainsäädäntö lähtee siitä, että jos henkilötietoja luovutetaan EU/ETA-alueen ulkopuolelle ("kolmansiin maihin"), tulee tietojen luovuttajan varmistaa, että henkilötiedot nauttivat kohdemaassa yhtä korkeasta suojasta kuin EU/ETA-maissa. On

<sup>13</sup> Kun työsuhte tai asiakassuhde päättyy, peruste henkilötietojen käsittelemiselle päättyy ja henkilötiedot tulee lain mukaan poistaa. Niinpä itse asiassa jo henkilötietolaistakin seuraa, että käyttäjän käyttäjätunnukset organisaation tietojärjestelmiin pitää sulkea kun työsuhte, asiakassuhde tai henkilön muu asiallinen yhteys organisaation toimintaan päättyy.

joukko maita (esimerkiksi Sveitsi ja Argentiina), joissa EU-komissio on todennut jo lainsäädännön takaavan riittävän suojan henkilötiedoille. Jos henkilötietoja kohdemaassa suojaava tietosuojalainsäädäntö on kuitenkin EU-lainsäädäntöä heikompi, on henkilötietojen luovuttajan varmistettava sopimuksella, että luovutetuille henkilötiedoille taataan kohdemaassa EU-tasoinen tietosuoja.

Esimerkiksi Yhdysvaltojen tietosuojalainsäädäntö ei perustu OECD:n tietosuoja-periaatteisiin, eikä henkilötietoja voida automaattisesti luovuttaa EU/ETA-maista Yhdysvaltoihin. Yhdysvaltojen kauppaministeriö ja EU-komissio ovat kuitenkin sopineet Safe Harbour –nimisestä järjestelystä, jonka piiriin ilmoittautuneet yhdysvaltalaiset yritykset ovat vapaaehtoisesti sitoutuneet EU-vaatimukset täyttävään tietosuojan noudattamiseen.

Kannattaa kuitenkin muistaa, että tietosuojalainsäädäntö ja Safe Harbour –järjestely koskee vain henkilötietojen siirtämistä kahden rekisterinpitäjän välillä. Jos loppukäyttäjä omin päin siirtää omia henkilötietojaan EU:n ulkopuolelle – esimerkiksi perustaa itselleen tilin yhdysvaltalaisen yrityksen palvelimelle – eivät hänen henkilötietonsa lähtökohtaisesti ole lainkaan eurooppalaisen tietosuojalainsäädännön piirissä.

## 9.6. Pohdittavaa

- Henkilötietolain mukaan henkilötiedolla tarkoitetaan *kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi*. Luvussa 3.4 esiteltiin pseudonyymien käsite. Täyttääkö pseudonyymi tunniste (esimerkiksi timo99) henkilötiedon määritelmän?
- Käyttäjä suorittaa federoidun kirjautumisen (luku 8), jolloin hänen kotiorganisaationsa luovuttaa hänen henkilötietojaan toiselle rekisterinpitäjälle, joka ylläpitää tunnistukseen nojaavaa palvelua. Mitä kaikkea tulee huomioida, jotta luvussa 9.1 esitetyt vaatimukset saadaan henkilötietoja luovutettaessa täytettyä?
- Henkilötietojen käsittelyn perustaminen rekisteröidyn suostumukseen edellyttää, että suostumus on vapaasti annettu – toisin sanoen rekisteröityä ei millään tavalla painosteta suostumuksen antamiseen. Missä määrin suostumusta voidaan käyttää henkilötietojen luovuttamisen perusteena silloin, kun yrityksen työntekijä joutuu työtehtävissään suorittamaan federoidun kirjautumisen toisen organisaation extranet-palveluun.



Tampereen teknillinen yliopisto  
PL 527  
33101 Tampere

Tampere University of Technology  
P.O.B. 527  
FI-33101 Tampere, Finland